Adding @Donn's reply sent by private message:

Hm, for some reason my post wasn't saved. Well, here we go again :-) :

I managed to install and (almost) configure everything properly. Remember, all Talend components are in independent containers, though on the same

1. When I go to the DataPrep Website, I get redirected to IAM in order to log in. However, I get redirected to "localhost", like that:
http://localhost:9080/idp/federation?wa=wsignin1.0&.....

When I change localhost to docker-dev-52.cgn.company.com, I get redirected to IAM. After logging in with the data prep user I have created in TAC,

The IAM log shows the following:

2018-02-23 19:41:20.878 -ERROR [http-nio-9080-exec-9] o.a.c.f.s.i.b.EndpointAddressValidator   : The endpointAddress value of http://docker-dev-52

I found a similar issue in the Talend Knowledgebase: https://community.talend.com/t5/Installation/Authentication-failed-in-Data-Stewardship/ta-p/3

However, this is for Data Stewardship, but I still tried it out - no luck. Here is my curent config:

IAM: iam.properties:

```
tac.url=http://docker-dev-52.cgn.company.de:8080/org.talend.administrator-6.4.1/
tac.user-name=security@company.com
tac.password=XvHOgly6990XI3t4NVPN+g==
tac.application=DataPrep

# ------------------------------------------------------------------------------
# IMPORTANT:
# Change of these 2 variables requires deleting both oidc and idp databases
# ------------------------------------------------------------------------------
iam.host=docker-dev-52.cgn.company.de
iam.url=http://${iam.host}:9080
```

```
# IDP Settings
idp.url=${iam.url}/idp
idp.db.url=jdbc:h2:${CATALINA_HOME}/idp/idpdb;DB_CLOSE_DELAY=-1
idp.db.driverClassName=org.h2.Driver
idp.db.username=idp
idp.db.password=6zQsVb2TNlehmcBHS+E2qQ==
idp.db.defaultData=true
idp.db.platform=H2Dictionary

# OIDC Settings
oidc.url=${iam.url}/oidc
oidc.host=${iam.host}
oidc.issuer=accounts.talend.com
oidc.db.driverClassName=org.h2.Driver
oidc.db.url=jdbc:h2:${CATALINA_HOME}/oidc/oidcdb;DB_CLOSE_DELAY=-1
oidc.db.username=oidc
oidc.db.password=nL9phBqQQtb5iAu9f6uEUg==
oidc.db.databasePlatform=org.apache.openjpa.jdbc.sql.H2Dictionary
oidc.db.dialect=org.hibernate.dialect.H2Dialect
oidc.accessTokenLifetime=3600
oidc.dynRegService.initialAccessToken=S3hmqC5Q7SlGwmrfq190EA==
oidc.clientResources.pattern=file://${CATALINA_HOME}/clients/*.json

# STS Settings
sts.url=${iam.url}/sts-tac
sts.issuer=Fediz STS
sts.keystore.file=sts.jks
sts.keystore.password=l5j+/7FS8tiJUpU486CfxQ==
sts.keystore.alias=iam-sts-onpremise
sts.key.password=l5j+/7FS8tiJUpU486CfxQ==
sts.syncope.url=${iam.url}/sts
syncope.url=${iam.url}/syncope/rest
syncope.user-name=admin
syncope.password=S3hmqC5Q7SlGwmrfq190EA==

# SCIM Settings
security.oidc.client.keyUri=${oidc.url}/jwk/keys
security.oauth2.resource.tokenInfoUri=${oidc.url}/oauth2/introspect

# General Settings
log.path=${CATALINA_HOME}/logs
iam.config.encrypt=true

iam.additionalTLDs=lan,de,company,cgn,docker-dev-52

IAM / tdp-client.json:

{
  "post_logout_redirect_uris" : [ "http://docker-dev-52.cgn.company.de:9999", "http://localhost:9999", "http://127.0.0.1:9999" ],
  "grant_types" : [ "authorization_code", "refresh_token", "password" ],
  "scope" : "openid refreshToken",
  "client_secret" : "ef3+h0qm/1NSFfZX24TFAzIhWsvCjJmhlo6j05ktcho=",
  "redirect_uris" : [ "http://docker-dev-52.cgn.company.de:9999/signIn", "http://localhost:9999/signIn", "http://127.0.0.1:9999/signIn" ],
  "client_name" : "TDP DataPrep",
  "client_id" : "64xIVPxviKWSog"
```

}

DataPrep / application.properties:

```
#
# ============================================================================
# Copyright (C) 2006-2016 Talend Inc. - www.talend.com
#
# This source code is available under agreement available at
# https://github.com/Talend/data-prep/blob/master/LICENSE
#
# You should have received a copy of the agreement
# along with this program; if not, write to Talend SA
# 9 rue Pages 92150 Suresnes, France
#
# ============================================================================
#

#
# Security settings (using TAC):
#
# warning: the ending '/' is mandatory:
tac.url=http://docker-dev-52.cgn.company.de:8080/org.talend.administrator-6.4.1/
#
# Public IP:
# This is the public ip (or hostname) of the server hosting Data Prep server
#
public.ip=docker-dev-52.cgn.company.de
server.port=9999
iam.ip=docker-dev-52.cgn.company.de

# Async execution (leaves high value for large dataset support).
spring.mvc.async.request-timeout=300000

#
# Live datasets
#
# Data Prep will only list tasks with this prefix:
tac.task-prefix=dataprep_

# TAC user:
# It must have "Operation Manager" or "Designer" role, and have authorization on required projects to list tasks in "Talend job" datasets.
# It must have "Administrator" role in TAC, in order to list users and groups for sharing.
tac.user-name=dpadmin@company.de
tac.password=XvHOgly6990XI3t4NVPN+g==

#
# Mongodb settings
#
mongodb.host=localhost
```

```
mongodb.port=27017
mongodb.database=dataprep
mongodb.user=dataprep-user
mongodb.password=V4+wDTj9WTW5Qgr214HCXQ==
multi-tenancy.mongodb.active=true
# For more complex use cases, mongo.* configurations can be overridden by specifying URI directly:
mongodb.uri=mongodb://talend641-dev-mongodb:27017/dataprep

# Mongodb TLS settings
#
# mongodb.ssl=true
# mongodb.ssl.trust-store=/path/to/trust-store.jks
# mongodb.ssl.trust-store-password=trust-store-password
#
# HTTP TLS settings
#
# tls.key-store=/path/to/key-store.jks
# tls.key-store-password=key-store_password
# tls.trust-store=/path/to/trust-store.jks
# tls.trust-store-password=trust-store_password
# false to disable hostname verification
# tls.verify-hostname=false

security.provider=oauth2
security.token.secret=yZzHjE4PyAatbSY1/zj1vQ==
security.token.renew-after=30
security.token.invalid-after=3600

spring.profiles.active=server-standalone
spring.mvc.favicon.enabled=false

# Service documentation
service.documentation=false
service.documentation.name=Talend Data Preparation - API
service.documentation.description=This service exposes high level services that may involve services orchestration.
service.paths=api

# size limit for dataset in lines (if dataset.lines > limit, dataset is truncated)
dataset.records.limit=10000
dataset.local.file.size.limit=2000000000
dataset.imports=local,job,tcomp-JDBCDatastore,tcomp-SimpleFileIoDatastore,tcomp-SalesforceDatastore,tcomp-S3Datastore
dataset.list.limit=10

# Address of the data set service (set at runtime by unit tests depending on random port)
dataset.service.url=http://${public.ip}:${server.port}
transformation.service.url=http://${public.ip}:${server.port}
preparation.service.url=http://${public.ip}:${server.port}
fullrun.service.url=http://${public.ip}:${server.port}

# Configure all services for file storage
dataset.metadata.store=mongodb
# file or s3
preparation.store=mongodb
user.data.store=mongodb
folder.store=mongodb
upgrade.store=mongodb
```

```
# Cache management (location for cache and content storage)
content-service.store=local
content-service.store.local.path=data/

# Preparation service configuration (see preparation service)
preparation.store.remove.hours=24

# Lock on preparation (mongodb or none) delay in seconds
lock.preparation.store=mongodb
lock.preparation.delay=600

# Enable Hazelcast (true = enabled, false = disabled)
hazelcast.enabled=true

# Lucene index configuration
luceneIndexStrategy=singleton

#
# Asynchronous (full run / sampling) operations
#
# storage
execution.store=mongodb
# allowed concurrent runs
async.operation.concurrent.run=5

# TCOMP Server: deactivated if property is not present.
#tcomp.server.url=http://<place_tcomp_ip_here>:8989/tcomp

# hide some tcomp properties
# tcomp-JDBCDataset.sourceType.hide=true
# tcomp-JDBCDatastore.password.hide=true
tcomp-SimpleFileIoDatastore.kerberosPrincipal.default=${streams.kerberos.principal}
tcomp-SimpleFileIoDatastore.kerberosKeytab.default=${streams.kerberos.keytab_path}
tcomp-SimpleFileIoDataset.path.default=${streams.hdfs.server.url}

# remove test connection step from talend component form
tcomp-SimpleFileIoDatastore.test_connection.visible=false


# Full run task max execution time (max execution time for a full run in milliseconds)
# async.operation.watcher.ttl=3600000

# Max wait time when data prep waits for live data set input
# receivers.timeout=3600000
#
# Data Quality
#
# where indexes are extracted:
dataquality.indexes.file.location=data/data-quality/org.talend.dataquality.semantic
# display semantic types within dataprep UI
dataquality.semantic.list.enable=false
dataquality.server.url=<place_data-quality_server_url_here>

# to receive data quality updates
dataquality.semantic.update.enable=false
```

```
dataquality.event.store=mongodb
spring.cloud.stream.kafka.binder.brokers=<place_kafka_ip_here>
spring.cloud.stream.kafka.binder.zkNodes=<place_zookeeper_ip_here>
spring.cloud.stream.kafka.binder.defaultBrokerPort=9092
spring.cloud.stream.kafka.binder.defaultZkPort=2181
spring.cloud.stream.bindings.input.destination=${MESSAGING_DOCUMENT_QUEUE:dictionary}
spring.cloud.stream.bindings.input.content-type=application/x-java-object;type=org.talend.dataquality.semantic.model.DQDocumentAction
spring.cloud.stream.bindings.input.group=${MESSAGING_CATEGORY_GROUP:dictionaryGroup}
spring.cloud.stream.bindings.category.destination=${MESSAGING_CATEGORY_QUEUE:category}
spring.cloud.stream.bindings.category.content-type=application/x-java-object;type=org.talend.dataquality.semantic.model.DQCategoryAction
spring.cloud.stream.bindings.category.group=${MESSAGING_REGEX_GROUP:dictionaryGroup}
spring.cloud.stream.bindings.regEx.destination=${MESSAGING_REGEX_QUEUE:regex}
spring.cloud.stream.bindings.regEx.content-type=application/x-java-object;type=org.talend.dataquality.semantic.model.DQCategoryAction
spring.cloud.stream.bindings.regEx.group=${MESSAGING_REGEX_GROUP:dictionaryGroup}
data.management.lucene.documents.folder=${dataquality.indexes.file.location}/index/dictionary
data.management.lucene.categories.folder=${dataquality.indexes.file.location}/category
data.management.receiving.folder=${dataquality.indexes.file.location}/index/received/
data.management.regex.folder=${dataquality.indexes.file.location}/regex

# Streams configuration
streams.enable=false
streams.flow.runner.url=http://<local machine ip>:<Big data preparation port>/v1
streams.kerberos.principal=<principal>
streams.kerberos.keytab_path=<keytab path>
streams.hdfs.server.url=hdfs://<host>:<port>/<filepath>

######################## SSO ##############
security.basic.enabled=false
security.oidc.client.expectedIssuer=accounts.talend.com
iam.license.url=http://${iam.ip}:9080/oidc/services
security.oidc.client.keyUri=http://${iam.ip}:9080/oidc/jwk/keys
security.oauth2.client.clientId=64xIVPxviKWSog
security.oauth2.client.clientSecret=1234567890qwertz
security.oidc.client.claimIssueAtTolerance=120
# security.oauth2.resource.serviceId=${PREFIX:}resource
security.oauth2.resource.tokenInfoUri=http://${iam.ip}:9080/oidc/oauth2/introspect
security.oauth2.resource.uri=/api/**,/folders/**,/datasets/**,/preparations/**,/transform/**,/version/**,/acl/**,/apply/**,/export,/export/**,/agg
security.oauth2.resource.filter-order=3
security.oauth2.resource.tokenInfoUriCache.enabled=true
security.scim.cache.enabled=true
security.scim.enabled=true

security.oauth2.client.access-token-uri=http://${iam.ip}:9080/oidc/oauth2/token
security.oauth2.client.scope=openid refreshToken
security.oauth2.client.user-authorization-uri=http://${iam.ip}:9080/oidc/idp/authorize?prompt=none
security.oauth2.sso.login-use-forward=false
server.session.cookie.name=TDPSESSION
security.sessions=stateless
security.user.password=none

# SSO logout properties for dataprep API & Gateway
security.oidc.client.endSessionEndpoint=http://${iam.ip}:9080/oidc/idp/logout
security.oidc.client.logoutSuccessUrl=http://${public.ip}:${server.port}
security.oauth2.logout.uri=/signOut
security.oauth2.sso.login-path=/signIn
```

```
iam.scim.url=http://${iam.ip}:7777/scim/
####################### SSO ##############

gateway-api.service.url=http://${public.ip}:${server.port}
gateway-api.service.path=/gateway

zuul.servletPath=/gateway/upload

zuul.routes.dq.path=/gateway/dq/semanticservice/**
zuul.routes.dq.sensitiveHeaders=${zuul.sensitiveHeaders}
zuul.routes.dq.url=${dataquality.server.url}/
proxy.auth.routes.dq=oauth2

zuul.routes.api.path=/gateway/api/**
zuul.routes.api.sensitiveHeaders=${zuul.sensitiveHeaders}
zuul.routes.api.url=http://${public.ip}:${server.port}/api
proxy.auth.routes.api=oauth2

zuul.sensitiveHeaders=Cookie,Set-Cookie,Expires,X-Content-Type-Options,X-Xss-Protection,Cookie,X-Frame-Options,Cache-control,Pragma

zuul.host.socket-timeout-millis=300000
zuul.host.connect-timeout-millis=5000

############# LOGGING #############
## Path of the log file
logging.file=data/logs/app.log
## Level output pattern, uncomment to add the MDC user after level
logging.pattern.level=%5p [user %X{user}]
## Pattern used for file logging, uncomment to override Spring default
#logging.pattern.file=%d{yyyy-MM-dd HH:mm:ss.SSS} %5p --- [%t] %-40.40logger{39} : %m%n%wEx
## Data-Prep loggers
logging.level.=WARN
logging.level.org.talend.dataprep=INFO
logging.level.org.talend.dataprep.api=INFO
logging.level.org.talend.dataprep.dataset=INFO
logging.level.org.talend.dataprep.preparation=INFO
logging.level.org.talend.dataprep.transformation=INFO
logging.level.org.talend.dataprep.fullrun=INFO
logging.level.org.talend.dataprep.api.dataquality=INFO
logging.level.org.talend.dataprep.configuration=INFO
To recap:

Issue 1: Redirect to localhost instead of docker-dev-52.cgn.company.de

Issue 2: Login fails due to error (message) in IAM



Thanks for the help so far!
```

@asharma, @fhuaulme, @sm, can you help on that one?

BTW, @Donn: thank you for pointing out the gap in the product documentation regarding the IAM <=> TAC configuration. I've brought it up to our documentation team and it will get fixed soon enough.

Regards,

Gwendal