IBM App Connect Enterprise Manufacturing pack

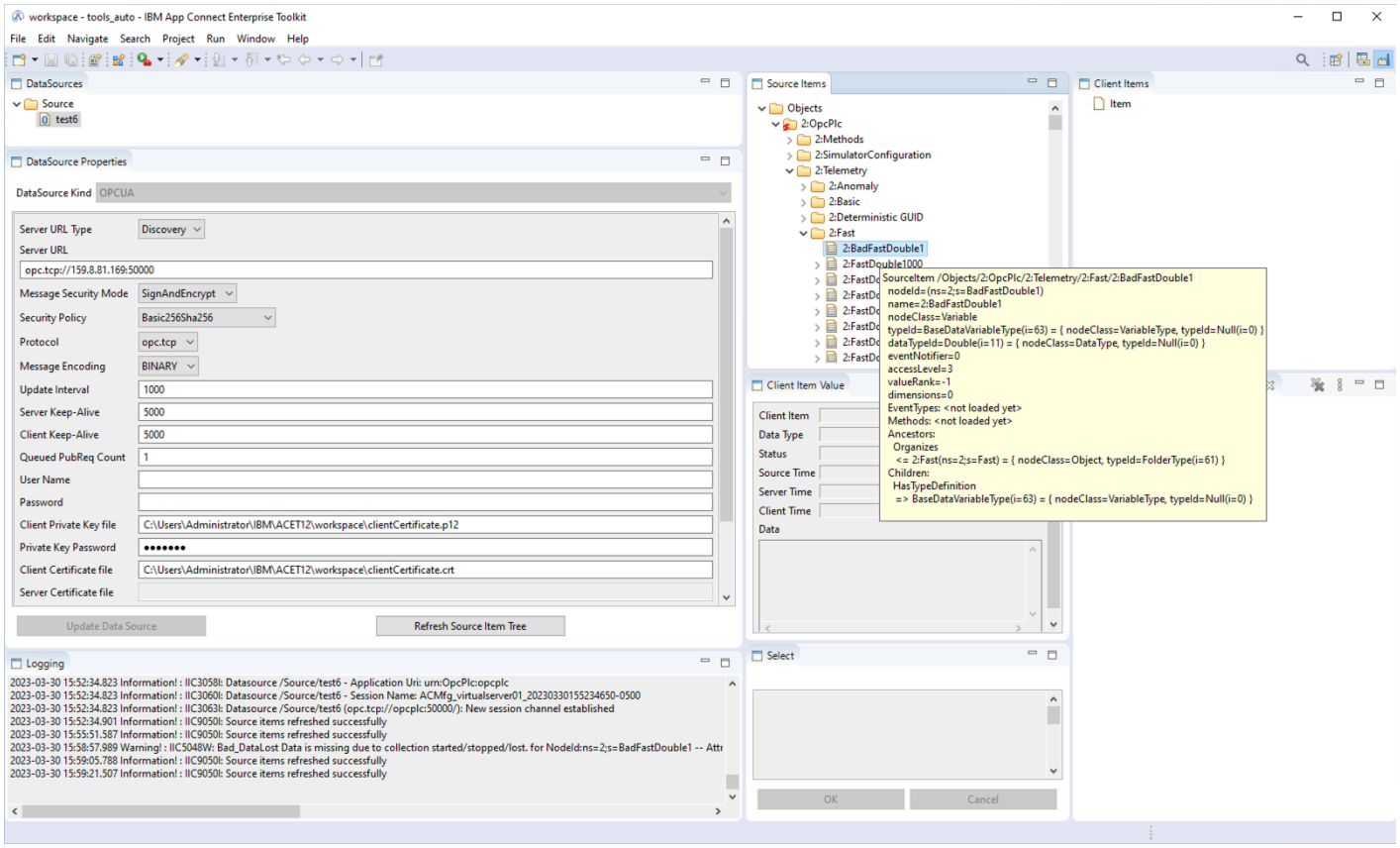
Laurent MARTIN

2023/05/10

Contents

Chapter 1

General



IBM ACE is available with an extension supporting the OPC UA interface, as a client, called here" ACMfg (App Connect Enterprise for Manufacturing).

For testing purpose an OPC UA server (generating samples) is needed. We can use the OPC PLC server.

The communication can be either un-encrypted (for tests only) or encrypted, but in that case a X509 certificate must be put in place (both sides).

Linux UNIX

Note: The `Makefile` is intended to be run on a Unix-like system (macOS, Linux)

Windows

In the following sections, `$HOME` refers to `%USERPROFILE%` on Windows.

A IBM Performance Report for ACMfg is available.

Chapter 2

Scripts and initialization

A Makefile and scripts are provided.

Before using the scripts and the `Makefile`, first initialize the config, execute:

```
make init
```

This create a configuration file: `private/configuration.env` from the template: `configuration.tmpl.env`.

Both the Makefile and scripts rely on `private/configuration.env` (shell variables). `generated/configuration.mak` is generated from the configuration and used in the `Makefile`.

The required values for the configuration parameters are commented in the template and later in this document.

Chapter 3

Security and Encryption

3.1 Generation of Client Certificate

The OPC-UA protocol requires mutual authentication and supports encryption. Optionally, for tests, clear transmission can be used.

Prior to configuring the ACMfg, one needs to generate a certificate.

In production, Security will be used, this requires certificates on both the client and server.

The ACE documentation provides the steps to generate a self-signed certificate.

The `Makefile` provided here generates a simple self-signed certificate in the required format. It follows the manual steps described in the documentation.

Edit the file `private/configuration.env`: set the private key password.

To generate the certificate and key:

```
make
```

Generated files are located in folder `generated`:

- `clientCertificate.p12` : Private key and certificate protected by a password in a PKCS12 container.
- `clientCertificate.crt` : The certificate alone in PEM format.

3.2 Comments on ACMfg documentation

A few comments on the ACE documentation:

- The ACMfg OPC UA client requires: The certificate's Private Key, the Key's passphrase, and the certificate.
- The documentation provides the steps to generate those. (used in the Makefile)
- The ACMfg toolkit UI talks about "PEM" format for both.
- The method proposed in documentation shows a PKCS12 container is generated.
- The UI tells, for the key: **Client Private Key in pem file (BASE64)**

In fact, the values to provide are:

- **Client Private Key file** : Expects the PKCS12 container, not PEM BASE64
- **Private Key password** : the password for the PKCS12 container
- **Client Certificate file** : The certificate in PEM format

If the key is not provided in the PKCS12 container, then the following error is logged:

```
ERROR! IIC2037E: Caught exception when trying to load the client certificate and key from C:\...\clientCertif
```

The content of the PKCS12 container (with both the key and certificate) can be displayed with:

```
openssl pkcs12 -info -in generated/clientCertificate.p12 -nodes -password pass:_pass_here_
```

Chapter 4

OPC PLC simulator server

In order to simulate sensors, a simulator can be used. We use here the OPC PLC server.

4.1 Installation of client certificate

The current working directory in the container is : `/app`, as can be seen in the log once the simulator is started:

```
[INF] Current directory: /app
...
[INF] Application Certificate store path is: pki/own
...
[INF] Trusted Issuer Certificate store path is: pki/issuer
...
[INF] Trusted Peer Certificate store path is: pki/trusted
...
[INF] Rejected Certificate store path is: pki/rejected
```

So, the default folders used in the container are:

```
/app
   /pki
      /own
      /issuer
      /trusted
      /rejected
```

If no server certificate is provided, the server generates a self signed certificate containing the hostname (of the container, so we fix the hostname value on container startup) in `/app/pki/own`.

Edit configuration.env and set the address of the OPC PLC VM: `opcua_server_address` The execute:

```
make deploy_opcplc
```

It will do the following:

- On the OPC PLC VM, in the user's home, a folder `pki` is created
- Copy the file `clientCertificate.crt` and `start_opc.sh` into it.

Later, when the container is started, a volume is created to map this `pki` folder in the user's home to the `/app/pki` folder in the container. The simulator is given the path to the client certificate (in the container) to add it to the trusted store.

4.2 Startup

The startup script is provider for convenience: `start_opc.sh`

Several parameters are provided to allow unencrypted use, trust of client cert, fix the container hostname.

4.3 Server certificate

Upon startup, the server will generate a self-signed certificate if none is already provided.

The server runs in the container, which has a hostname defaulting to the container id. The CN of the certificate is generated with the hostname, but that hostname changes upon each start of the container (container id), this will make subsequent start fail due to the changing name. The solution used is to fix fix the container host name, so that the generated server certificate can be re-used. (in case we need it on the client side).

Chapter 5

ACE Manufacturing

ACMfg provides a manufacturing view with the following tabs:

- `DataSources`
- `DataSource Properties`
- `Logging`
- `Source Items`
- `Client Item Value`
- `Select`
- `Client Items`
- `Client Item Properties`

Note: (IMPORTANT) The values shown in `DataSource Properties` are the ones for the data source selected in `DataSources`

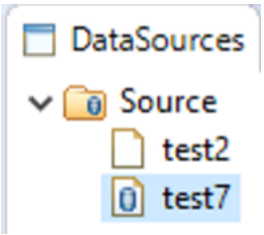
Note: (IMPORTANT) Similarly, later when we create the Item mappings, it is important to select the Item in tab `Client Items` so that buttons in tab `Client Item Properties` are activated.

5.1 Creation of Data Source

In the `DataSources` tab is located the root source, named `Source`. This name can be changed.

Sources can be configured in a hierarchical manner, i.e. sub nodes can be created under the root node or another node.

Then any source node can be configured with a server connection: select the source and enter configuration in the `DataSource Properties` tab.



Here, I will use the default mapping node `Source`

Select `Source` in `DataSources` (click on it) for the configuration of the data source.

Note: Once configured, in next section, the source get a blue icon inside.

5.2 Configuration of DataSource without Encryption

For testing purpose **only**, it is possible to register a source server without encryption and authentication. This is much simpler than using certificates.

Note: The configuration of the startup script `start_opc.sh` allows connection from client without encryption. (option `--unsecuretransport`)

In `DataSource Properties` enter these values:

- **Message Security Mode** : None
- **Security Policy** : None
- **Client Private Key file** : leave empty
- **Private Key password** : leave empty
- **Client Certificate file** : leave empty

5.3 Configuration of DataSource with Encryption

Copy the generated files: `generated/clientCertificate.crt` and `generated/clientCertificate.p12` to the ACE workspace.

In `DataSource Properties` enter these values:

- **Message Security Mode** : `SignAndEncrypt`
- **Security Policy** : `Basic256Sha256`
- **Client Private Key file** : `[path to workspace]/clientCertificate.p12`
- **Private Key password** : the password used for the PKCS12 container
- **Client Certificate file** : `[path to workspace]/clientCertificate.key`

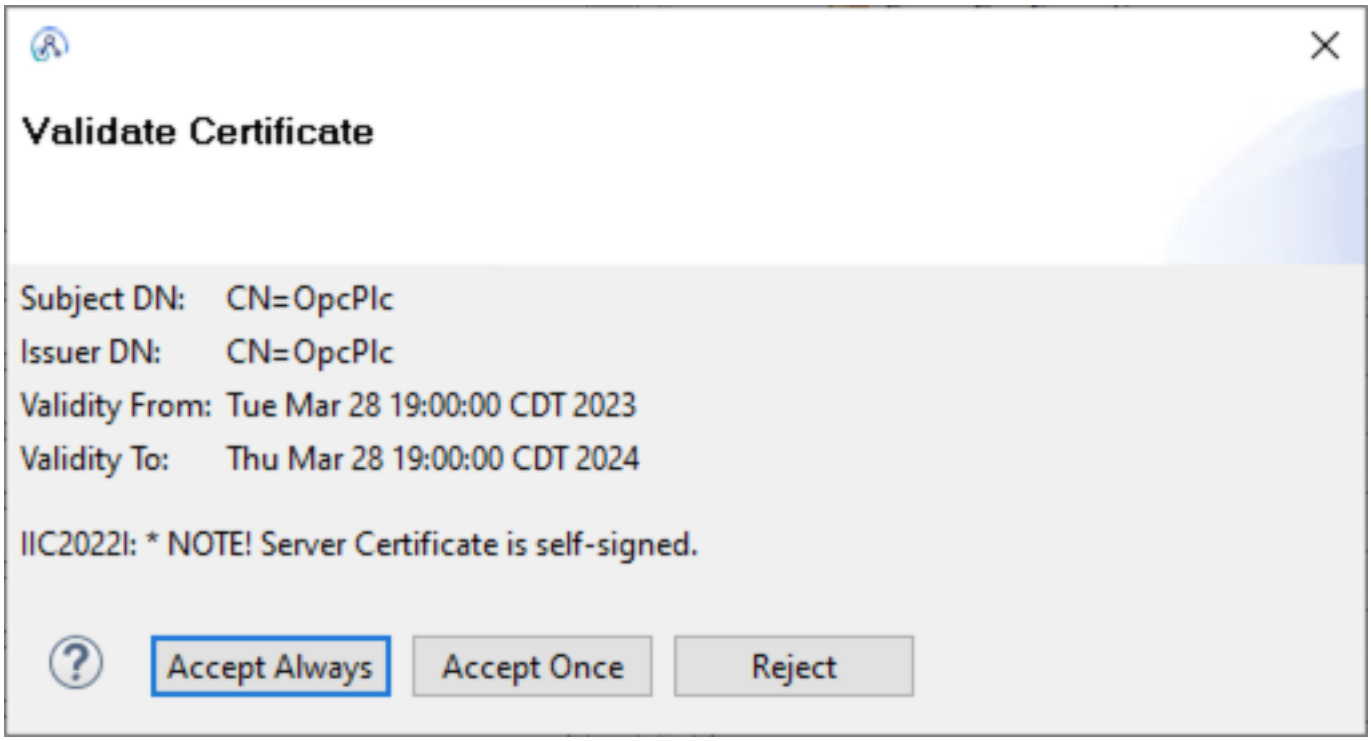
By default, the main folder for ACMfg is: `$HOME/.acmfg`

Upon configuration, the following file is generated: `$HOME/.acmfg/mappings/datasources.json`

Note: Take a note of the data source mappingPath, e.g. `/Source`: it will be needed to build the name of the PKCS12 password in the vault. It is the value of field `mappingPath` in `datasources.json`, noted `$source_mapping_path`.

5.4 Server certificate on client

The ACE OPC UA client allows (for testing) to accept the server certificate manually upon connection:

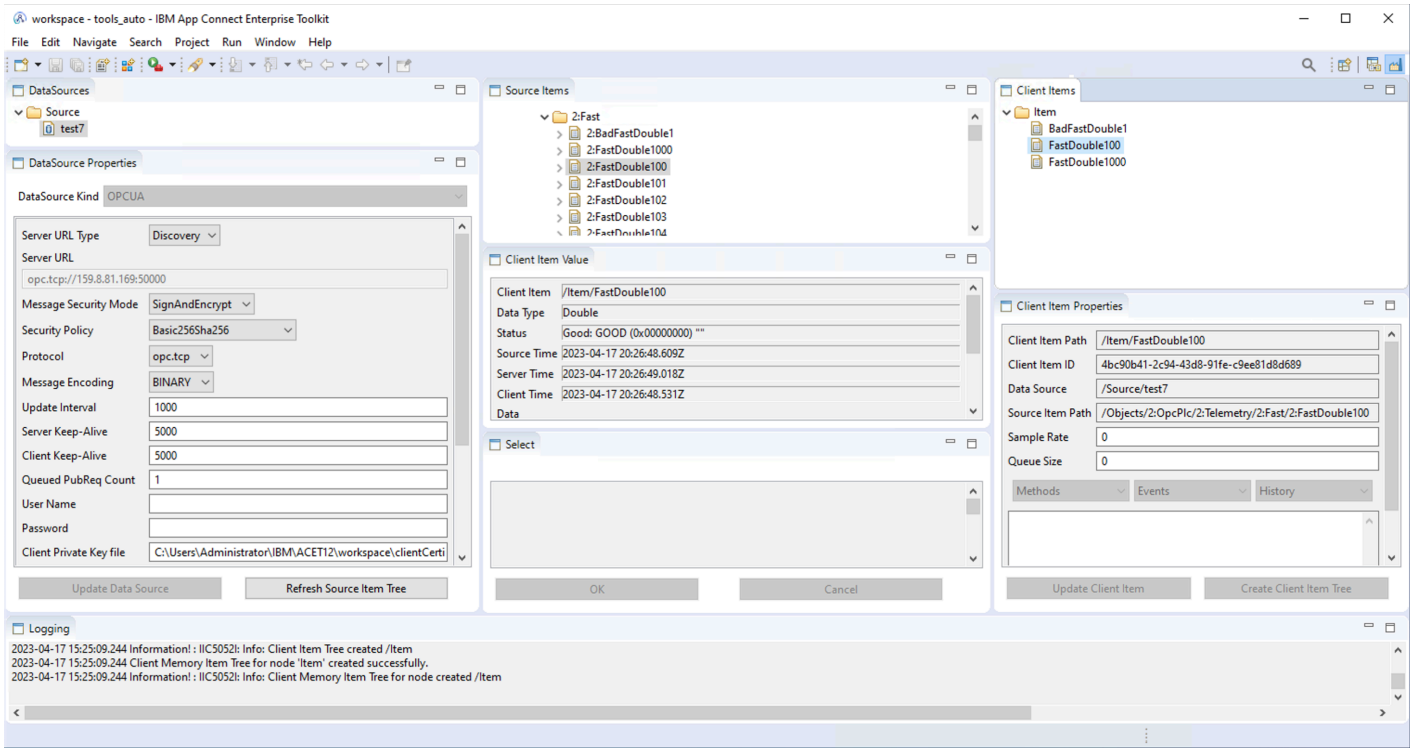


Once accepted the certificate is stored in `$HOME/.acmfg/PKI/CA/certs` (in DER format)

5.5 Preparation of mapping nodes

In the manufacturing view, follow these steps:

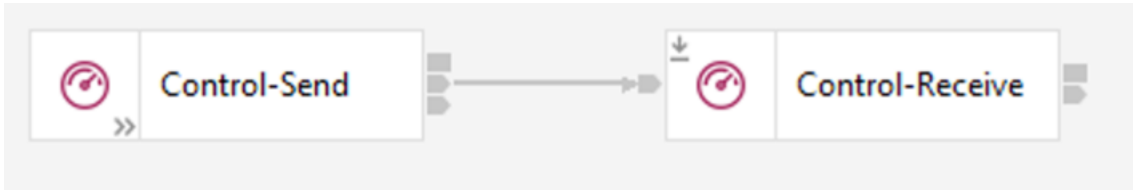
ACMfg Window Tab	Action
`DataSources`	Select the data source
`DataSource Properties`	Check that it is properly configured and connected. Click on `Refresh Source Item Tree`
`Source Items`	Check that items were retrieved.
`Client Items`	Select the element `Item`: it is the root item (it can be renamed).
`Source Items`	Navigate to Objects→OpcPlc→Telemetry. Select either a full section, or a list of source items, or a si
`Client Item Properties`	The button `Create Client Item Tree` becomes available (multiple selections), or `Create Client I`
`Client Items`	Note that items are now mapped under the selected item: `Item`.



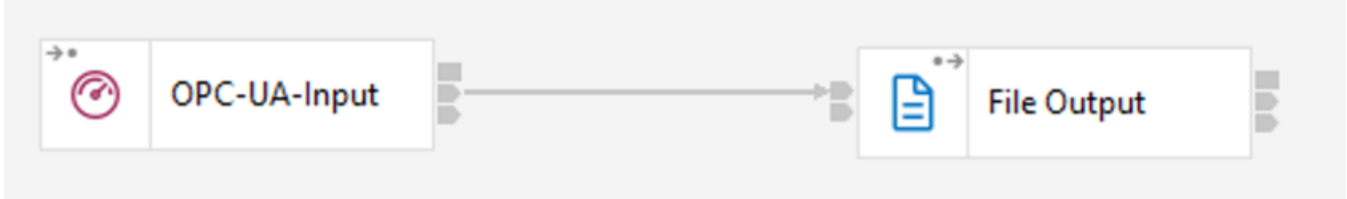
Upon configuration, the following file is generated: `$HOME/.acmfg/mappings/mapping_851eeb72-f996-4af4-8d63-d55c586c2826.`

5.6 Flow creation

As specified in the documentation, create one flow with both control nodes:



And a simple input flow can be:



To select sources for the OPC-UA-Input node follow this:

- in the connector configuration click on `Add`, this switches to the manufacturing view
- in `Client Items` select the desired items
- in `Select`, button `Add Trigger Item` is activated, click on it
- Eclipse switches back to the designer view.

Chapter 6

ACE: Starting the development `IntegrationServer` in the toolkit

Create an `IntegrationServer` in the toolkit: Set a password for the Vault (same as in `configuration.env`).

6.1 ACMfg jars

The `IntegrationServer` (or node) needs to be equipped with the ACMfg jar. This is described in the documentation. Edit `server.conf.yaml`, and configure like this (e.g on Windows):

```
ConnectorProviders:
  ACMfg:
    connectorClassName: 'com.ibm.industrypack.industryclient.connector.ICConnectorFactory'
    jarsURL: 'C:/Program Files/IBM/ACMfg/3.0.1.1/runtime/amd64_nt_4'
    property1: 'trustCertificate=true;isHA=false'
```

Note: Update the jar path accordingly to the actual version installed.

Properties are described here.

The property: `trustCertificate=true` means that an unknown certificate from a server will be automatically added to the list of accepted certificates.

6.2 Vault and secrets

The `IntegrationServer` also needs the certificate and private key. A vault can be used. If the vault was not created when the `IntegrationServer` was created using toolkit, then it can also be created subsequently. The `IntegrationServer` must be shutdown to create the vault.

See documentation

The vault is created in the `IntegrationServer` work dir: `[work_directory]/config/vault/store.yaml`

Windows

Open an ACE Console.

Example of workdir of `IntegrationServer`: `$HOME/IBM/ACET12/workspace/TEST_SERVER`

Linux UNIX

On Unix-like systems, open a terminal.

On Windows or Unix-like:

```
mqsivault --work-dir [work_directory] --create --vault-key [vault_key_name]
```

Build the `[credential_name]` like this: `$source_mapping_path/acmfgPrivateKeyUser`, e.g. `/Source/acmfgPrivateKeyUser`

Add the credential to the Vault:

```
mqsicredentials --work-dir [work_directory] --vault-key [vault_key_name] --create --credential-type ldap --cr
```

> **Note:** The `username` parameter is not used.

When the `IntegrationServer` is started it will look for that password based on `$source_mapping_path`.

TODO: Change: The data source server information is read from `$HOME/.acmfg`, including the certificate, private key.

Chapter 7

ACE: Starting the `IntegrationServer` in a container using the pre-built image

The idea here is to use the pre-built ACE container and provide ACMfg jars in the mounted volume.

> **Note:** Alternatively, it is also possible to create a custom container image.

To be able to pull pre-built images from the IBM registry, get your `entitlement_key` from My IBM Product Services. Edit the file: `private/configuration.env` and place your entitlement key.

Set a random secret for the `IntegrationServer` vault in `vault_key`.

```
make deploy_ace
```

This generates the client certificates, if needed, and sends the necessary files to the container host for integration server `ace_server_address`.

7.1 Creation and configuration of container

Then, on the VM where `podman` will be used, load the tools:

```
./deploy_acmfg.sh
```

This script performs the following steps:

- load configuration (from `configuration.env`) and helper functions

  ```
  source ace_container_tools.rc.sh
  ```

- Login to IBM image repository

  ```
  podman login cp.icr.io -u cp --password-stdin <<< $entitlement_key
  ```

- Work directory: Creation Ref.: ACE Doc.: mqsicreateworkdir

  Since we will mount an empty folder from the host, we must initialize the work directory for the `IntegrationServer` using `mqsicreateworkdir`:

  ```
  mkdir -p $ace_container_work_directory
  chmod 777 $ace_container_work_directory
  mqsicreateworkdir $ace_container_work_directory
  ```

- Vault: Creation

  Ref.: Youtube: Storing encrypted security credentials in a vault Ref.: ACE Doc.: mqsivault Ref.: ACE Doc.: mqsi-credentials

  Create an empty vault in the `IntegrationServer` work dir:

  ```
  mqsivault --work-dir $ace_container_work_directory --create --vault-key $vault_key
  ```

Note: Any operation on vault **can** be done while `IntegrationServer` is stopped. When `IntegrationServer` is stopped the vault key **must** be provided on command line (option `--vault-key $vault_key`).

Note: Some operations **must** be done while `IntegrationServer` is stopped: Creation of vault, deletion of entry.

Note: Some operations on vault **can** be done while `IntegrationServer` is running: List entries, Add entry. When `IntegrationServer` is running the vault key is not needed on command line: Requests are made through the `IntegrationServer`.

- Add Private Key password

  Credentials (username/password, and sometimes client id and secret) are sensitive pieces of information. A good practice is to store them in a safe location. ACE provides several ways to store credentials:

provider	description	doc
servercredentials	server.conf.yaml	doc default and override
setdbparms	in a parameter storage	can be played with file setdbparms.txt
vault	in an encrypted vault	

  Use the same command as previously with local server to create the credential in the Vault:

```
mqsicredentials \
--work-dir $ace_container_work_directory \
--vault-key $vault_key \
--create \
--credential-type ldap \
--credential-name $source_mapping_path/acmfgPrivateKeyUser \
--username not_used \
--password "$pkcs12_key"
```

- Add ACMfg

  Copies the following in the shared folder with container:

  - server.conf.yaml
  - ACEmfg jar files

7.2 Policies to override parameters

The location of the certificates for the OPCUA input node is copied from the data source JSON into the flow node configuration (and then lands in the bar file). This can be found in the XML description of the flow (`data.msgflow`). In order to override this value it is possible to use a policy.

Note: Other alternative: change the path in the bar file by editing the xml file of the flow.

Proceed as follows:

- Create a policy project, e.g. in the toolkit, here we use: `ContainerDeployment`
- Create a policy with the name equal to the **name** of the source. Not the path, but just the name of the source itself (node in tree). In case of doubt look at file `datasources.json`: it is the value of the field `"name"`. The name of the default source is `Source`
- Set the policy type to `User Defined`, and create two keys: `SECURITY_CLIENT_CERT` and `SECURITY_CLIENT_PRIV_KEY` with the path to those files inside the container.
- To tell the `IntegrationServer` to use this policy project, you can set the default policy project in `overrides/server.conf.yaml`. The generated file here sets that value to `ContainerDeployment`.

7.3 ACE: Create and Start container

- Ref.: ACE Doc.: `IntegrationServer` command

Several ports are to be published to allow access to the `IntegrationServer`:

port	Usage
7600	REST Administration port
7700	debug port
7800	user API port HTTP
7843	user API port HTTPS

The function `create_container_ace` from `ace_container_tools.rc.sh` is used:

```
source ace_container_tools.rc.sh

create_container_ace

podman start aceserver

podman logs -f aceserver
```

> **Note:** The container default entry point is overridden to allow additional arguments to be passed to the `IntegrationServer` (e.g. vault key). (It could also be provided through an environment variable, but not all options are available in env vars.)
>
> **Note:** The vault key is provided on the command line but can also be provided through an env var, or through a RC file. (Refer to the `IntegrationServer` manual)