Working with Cloudant NoSQL DB API

Prerequisites

This tutorial assumes that you know how to create MobileFirst native applications for iOS and Android, and that you have basic knowledge of adapter-based authentication. For more information, see the following tutorials:

- Configuring a native iOS application with the MobileFirst Platform SDK (../../hello-world/configuring-a-native-ios-with-the-mfp-sdk/)
- Creating your first native Android MobileFirst application (../../hello-world/creating-first-native-android-mobilefirst-application/)
- Adapter-based authentication (../../authentication-security/adapter-based-authentication/)

Overview

This sample is based on an IBM MobileFirst Platform Foundation technology that enables to store data for a mobile application: IBM MobileFirst Platform Cloudant Data Layer Local Edition. The Cloudant Data Layer Local Edition is an advanced NoSQL database which can handle a wide variety of data types, such as JSON, full-text, and geospatial data. This tutorial explains how to integrate and use the proper SDKs and APIs in iOS and Android MobileFirst applications.

This tutorial covers the following topics:

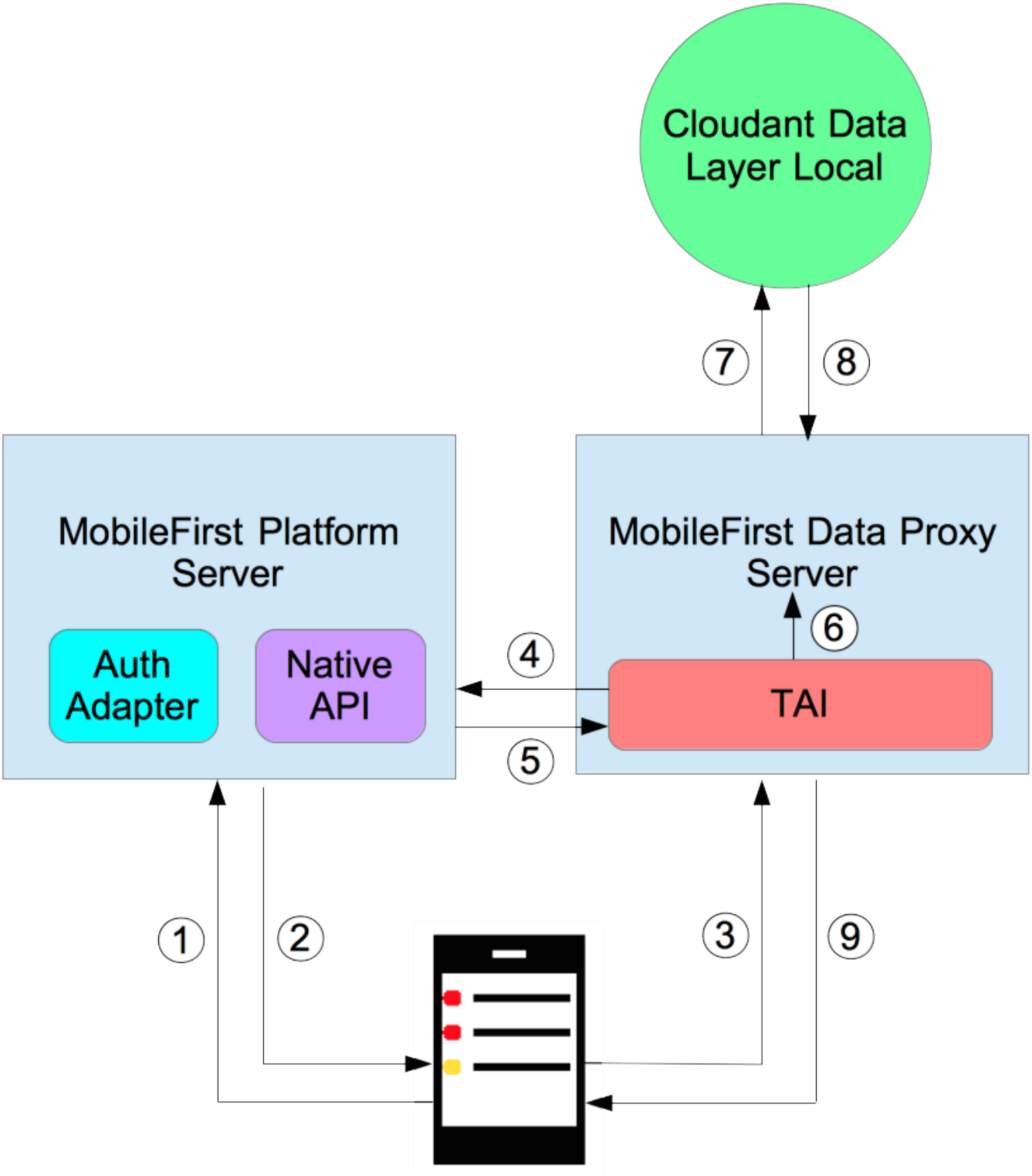
- Topology overview
- Setting up MobileFirst Data Proxy Server
- Setting up MobileFirst Server
- MobileFirst Platform Cloudant Data Layer Local
- Obtaining the sample
- iOS and Android client-side API tutorials

Topology overview

The attached sample integrates four major components for authentication, verification, and completion of operations against Cloudant Data Layer Local.

- MobileFirst Server: the runtime container for the application components (native APIs and the authentication adapter)
- MobileFirst Data Proxy Server: the proxy used to communicate with Cloudant Data Layer Local
- Cloudant Data Layer Local Edition: an advanced NoSQL database where application data can be stored
- MobileFirst OAuth Trust Association Interceptor: the front end for OAuth authentication of incoming requests to the MobileFirst Data Proxy

The following diagram shows the initial data request from Cloudant Data Layer Local via the mobile device. The process starts after the device receives an `401 unauthorized` error message when requesting a protected resource. The diagram does not show the entire OAuth process, but you can find more information in the topic about the OAuth-based security model, in the user documentation.



1. A request to a protected resource is sent from the mobile device to MobileFirst Server. In this sample, a request is made through adapter-based authentication with a basic username and password.
2. On valid authentication, a token is received and sent back to the device.
3. A request to receive data from the Cloudant Data Layer Local Edition is sent to the MobileFirst Data Proxy Server. This request is then intercepted by the MobileFirst OAuth Trust Association Interceptor (TAI). This request contains the token received in step 2.
4. The TAI sends a request to MobileFirst Server for validation.
5. The MobileFirst Authorization Server returns the public key for the TAI to validate the token.
6. The TAI forwards the now validated request to receive data to the MobileFirst Data Proxy Server.
7. The MobileFirst Data Proxy Server sends the request to the Cloudant Data Layer Local.
8. Cloudant Data Layer Local sends the requested information back to the MobileFirst Data Proxy Server.
9. The requested information is sent from the MobileFirst Data Proxy Server to the device.

Note: After the device has proper OAuth validation, it does not need to go back to MobileFirst Server to receive a new token for each request. The TAI validates the token against MobileFirst Server and when the token becomes invalid, a `401 unauthorized` error message is sent back to the device. When this occurs, the process starts over again and the device must re-authenticate with MobileFirst Server.

Setting up MobileFirst Data Proxy Server

If you have not installed and configured the MobileFirst Data Proxy, follow these instructions:

Installing and configuring the MobileFirst Data Proxy (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.installconfig.doc/install_config/t_installing_imf_datastore.html)

Whatever installation and configuration method you choose, make sure that the MobileFirst Data Proxy is configured to point to the Cloudant Local installation and to the MobileFirst Server instance.

- Installing the MobileFirst Data Proxy with Ant tasks (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.installconfig.doc/install_config/t_install_datastore_ant_tasks.html)
- Configuring WebSphere Application Server Liberty profile for MobileFirst Data Proxy manually (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.installconfig.doc/install_config/t_install_datastore_man_config_liberty.html)
- Configuring WebSphere Application Server full profile and WebSphere Application Server Network Deployment for MobileFirst Data Proxy manually (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.installconfig.doc/install_config/t_install_datastore_man_config_was.html)

MobileFirst OAuth Trust Association Interceptor

It is also mandatory to install the MobileFirst OAuth Trust Association Interceptor (TAI) to run the MobileFirst Data Proxy. Confirm that the TAI has been installed during the installation of the MobileFirst Data Proxy. If you have not done so, you can install it manually by following the Installing the MobileFirst OAuth Trust Association Interceptor (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.installconfig.doc/install_config/t_install_datastore_man_was_TAI.html) topic in the user documentation.

Setting up MobileFirst Server

The bluelist on premises project (https://hub.jazz.net/git/mobilecloud/mfp-bluelist-on-premises) contains a MobileFirst Platform sample. The sample includes a MobileFirst project with Native API applications for both iOS and Android (iOSBlueList and AndroidBluelist). It also includes the adapter used for authentication (CloudantAuthenticationAdapter). Deploy these artifacts to your MobileFirst Server instance.

You must set up authentication to the Cloudant Data Layer Local Edition by configuring access through the MobileFirst Data Proxy. For this purpose, it is required to integrate the OAuth capabilities that are provided by MobileFirst Platform.

In the sample, the `CloudantAuthenticationAdapter` adapter has been created and configured to handle this authentication. The `authenticationConfig.xml` file has also been modified to create a corresponding realm and login module as described in configuring OAuth security (http://ibm.biz/knowctr#SSHS8R_7.0.0/com.ibm.worklight.dev.doc/cloud/data/t_data_cloudantsec.html#oauth), in the user documentation.

MobileFirst Platform Cloudant Data Layer Local

In order to use this sample, you must install the IBM MobileFirst Platform Cloudant Data Layer Local Edition. For more information about the installation process, see IBM MobileFirst Platform Cloudant Data Layer Local Edition (http://www-01.ibm.com/support/knowledgecenter/SSTPQH_1.0.0/com.ibm.cloudant.local.install.doc/topics/clinstall_cloudant_local_overview.html), in the user documentation.

To obtain and download this component, see the following documentation:
Download the IBM MobileFirst Platform Foundation V7.0 products (http://www.ibm.com/support/docview.wss?uid=swg24039278)

Obtaining the sample

The sample that goes with the corresponding iOS and Android tutorials is hosted on the following jazzhub repository:

mfp-bluelist-on-premises (https://hub.jazz.net/git/mobilecloud/mfp-bluelist-on-premises)

You can clone the samples from IBM DevOps Services by running the following command in a directory of your choice:

```
$ git clone https://hub.jazz.net/git/mobilecloud/mfp-bluelist-on-premises
```

If you do not have `git` installed, follow the instructions on the git website (http://git-scm.com/downloads).