WSO2 API Manager 4.1.0 Fundamentals - Integration Profile

Management

WSO2 Training

Module Objective

At the end of this module, attendees will be able to:

- Understand how to use the Micro Integrator's command line tool (CLI).
- Understand how to use the Micro Integrator's dashboard.
- Understand the underlying management API that powers the CLI and monitoring dashboard.

Supporting Developer Tools

The following additional tools are available for managing and monitoring your integration deployments:

- Command Line Tool (CLI Tool)
- Monitoring Dashboard

Micro Integrator Command Line Tool

Using the Command Line Tool

The `./apictl mi` command in the CLI allows you to manage Micro Integrator artifacts. You can monitor the synapse artifacts (deployed in a specified Micro Integrator server) and perform various management and administration tasks from the command line.

- You need to download API Controller separately.
- Use `./apictl init` to get started with the API Controller and you can add environments and log in to them.
- Use the `./apictl mi` command to get the Micro Integrator runtime information and usage details.

Using the Command Line Tool

```
[{21-08-09 12:19}samuel:~/Downloads/apictl sam% ./apictl mi
Micro Integrator related commands such as login, logout, get, add, update, delete, activate, deactivate.

Usage:
  apictl mi [flags]
  apictl mi [command]

Available Commands:
  login       Login to a Micro Integrator
  logout      Logout from a Micro Integrator
  get         Get information about artifacts deployed in a Micro Integrator instance
  add         Add new users or loggers to a Micro Integrator instance
  delete      Delete users from a Micro Integrator instance
  update      Update log level of Loggers in a Micro Integrator instance
  activate    Activate artifacts deployed in a Micro Integrator instance
  deactivate  Deactivate artifacts deployed in a Micro Integrator instance

Flags:
  -h, --help   help for mi

Global Flags:
  -k, --insecure   Allow connections to SSL endpoints without certs
      --verbose    Enable verbose mode

Use "apictl mi [command] --help" for more information about a command.
```

Micro Integrator Dashboard

Micro Integrator Dashboard

- Monitor multiple Micro Integrator instances.
- View deployed artifacts**:**
  - View details of the artifacts deployed in a selected Micro Integrator instance.
- Update deployed artifacts**:**
  - Activate/deactivate artifacts from the dashboard.
  - Enable/disable tracing and statistics for artifacts.
- View logs.
- Update loggers and log levels.
- Manage users:
  - View and manage users in the external user store.

- Activate/deactivate the following artifacts from the dashboard: *Proxy Services*, *Endpoints*, and *Message Processors*.
- Enable/disable tracing and statistics for the following artifacts: *Proxy Services*, *Endpoints*, and *Message Processors*.

Managing User Access

The user credentials for signing in to the dashboard should be stored in your user store. This can be the default file-based user store or an external LDAP/RDBMS user store.
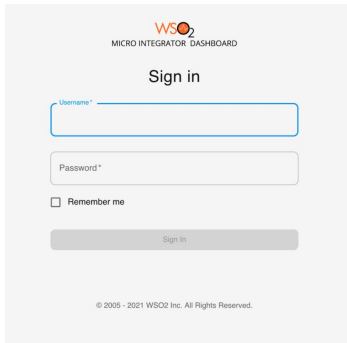
File-based user store:

```
[[internal_apis.users]]
user.name = "user-1"
user.password = "pwd-1"

[[internal_apis.users]]
user.name = "user-2"
user.password = "pwd-2"
```

Using the Micro Integrator Dashboard

- <u>Start the Micro Integrator dashboard</u>:
- Dashboard URL: *https://localhost:9743/dashboard.*

Using the Micro Integrator Dashboard

Micro Integrator Management API

Management API

- An internal REST API introduced as a substitute for admin services. This is enabled by default.
- Both the Micro Integrator dashboard and the CLI tool are powered by this internal REST API.
- Possible to directly access the management API for monitoring artifacts.
- Related documentation:
  - ⊙ Using the Management API.
  - ⊙ Securing the Management API.

Let's try it out!

Try CLI tool and MI Dashboard

Managing Users

Users in the Micro Integrator

WSO2 Micro Integrator requires **user** credentials for *authentication* and *authorization* purposes:

- Authentication of internal APIs.
- Authentication for integration use cases.
- Authorization for internal APIs.

Admin privileges allows you to add, remove users from an external user store.

- Use an existing admin user in the user store.

User Stores

- The Micro Integrator is shipped with a default **file-based** user store.
- You can **disable the file-based user store** and enable an external user store.
  - ◉ RDBMS user store
  - ◉ LDAP user store
- An external user store allows you to manage user from the **Dashboard** and **Command Line Tool**.
- JWT-based user authentication is enabled by default.

Let's try it out!

Managing Users