TAP User Management Documentation

TAP Version 0.8.0

Table of Contents

Terms and definitions

Term	Definition
CDH	Cloudera Hadoop
K8S	Kubernetes - orchestrator for containerized applications
POD	In K8S, a POD is a closely coupled set of containers that together form a logical machine.
UAA	User Account and Authentication Server, one of TAP components
User Role	Defines user's privileges in TAP

Overview

User Management is one of Trusted Analytics Platform (TAP) core components. Its main goal is to manage users and their roles on the platform.

Main functionalities

- Sending invitation emails
- Registration of users in the platform
- Removing users from the platform
- Changing user's roles

Deployment model

Since version 0.8 of TAP, deployment model assumes an existing K8S cluster combined with a CDH cluster. Therefore User Management is deployed as a POD on a Kubernetes node.

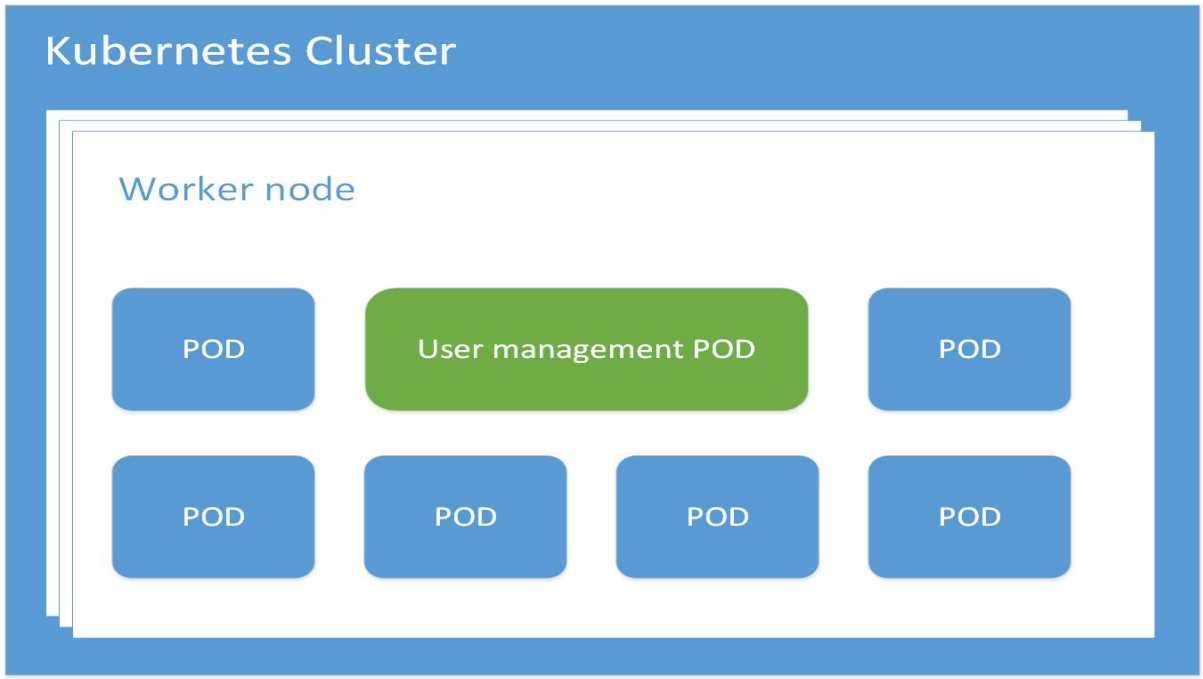


Figure 1. User Management in Kubernetes deployment

User Management POD

This POD consists of two containers:

- User Management application.
- RedisDB encrypted in-memory data structure store that stores invited users metadata and their security-codes required for registration. RedisDB is configured to use the built-in AOF persistency option and a CEPH volume as a persistence storage device.

Main differences between TAP 0.7 and TAP 0.8 versions

- Deployment model changed to the one using Kubernetes.
- In TAP 0.8 one organization w/o spaces is supported.
- There are only two user roles: regular user and admin user.

Architecture design

Cooperation with other components

As User Management needs to manage users and their roles, it needs to communicate with other TAP components: UAA and Auth Gateway.

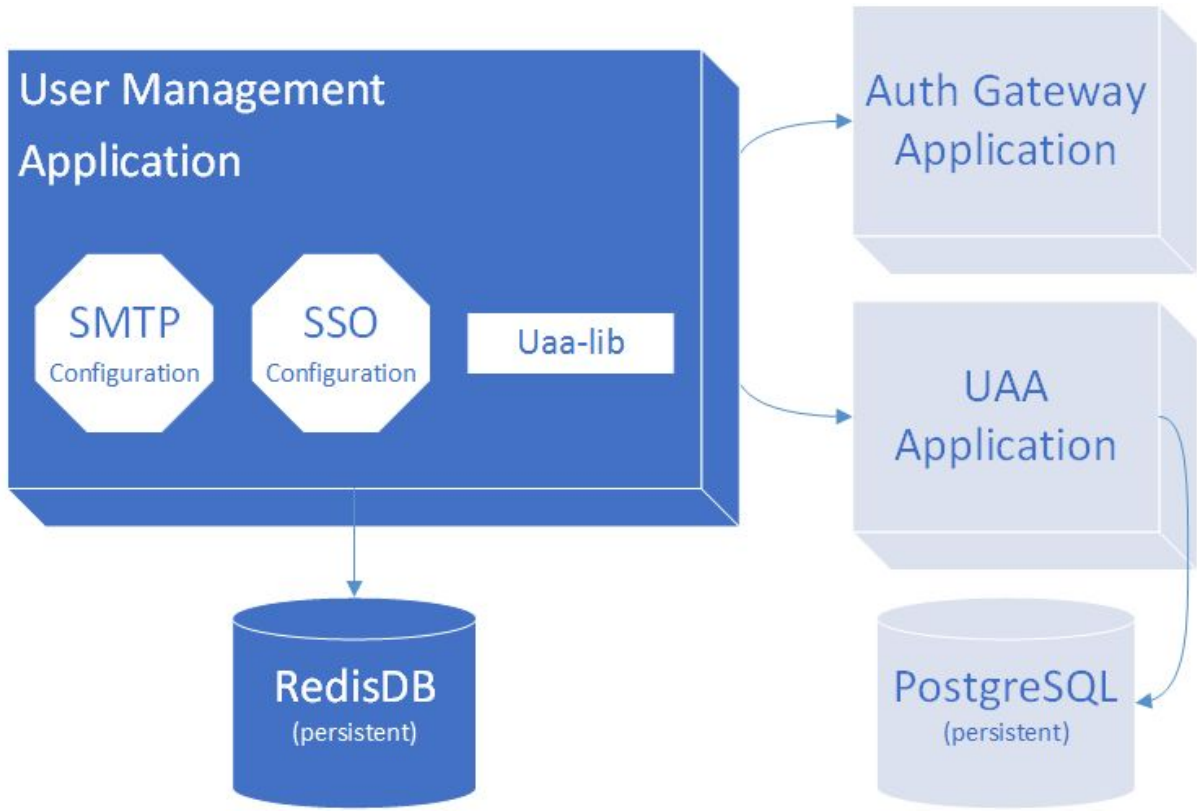


Figure 2. User Management components view

Auth Gateway

Auth Gateway is a TAP component that serves as a gateway for adding and removing authorization data for Hadoop components.

See details: https://github.com/trustedanalytics/auth-gateway

UAA

The UAA component has been developed as a part of the Cloud Foundry project, but it can also be used standalone. It acts as OAuth2 provider, coupled with user details persistence in database and a user management API. This is a key component in Platform security model and is responsible for distributing tokens. User management uses uaa-lib for communication with this component.

UAA also stores registered users data in an encrypted PostgreSQL database. The database uses CEPH volume for data persistency.

See details: https://github.com/trustedanalytics/uaa

Uaa documentation: https://github.com/trustedanalytics/uaa/tree/master/docs

User roles

Platform supports two different user roles: ADMIN and USER (regular). These roles are represented in the UAA database by the group to which user belongs (user belongs to tap.user or tap.admin group).

Regular user

Typical users of the TAP 0.8 system have access to:

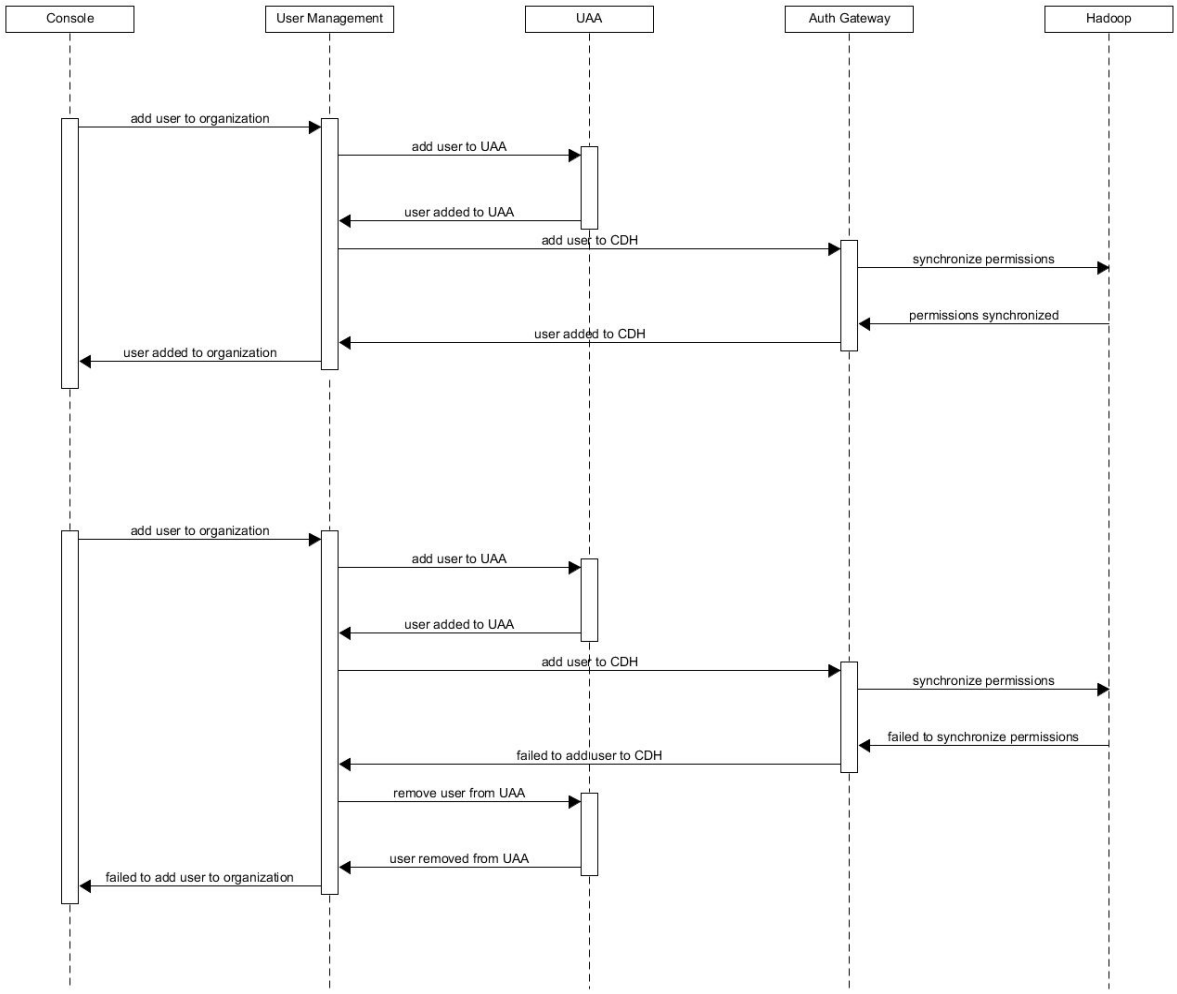
- Using the data science tools and other built-in services
- Deploying and running applications from artifacts
- Deploying and running applications from Docker images

Admin user

An *Admin* role has all the privileges of a regular user plus the ability to perform configuration and management actions for entities within their organization, such as:

- Adding/removing users
- Modifying platform's services offering by deploying/removing custom services

Add user sequential flow



API description

User Management API description is generated by Swagger plugin. It is available in User Management repository in folder "/docs" as json file. To read it:

1. Open online swagger files editor - editor.swagger.io.
2. Click 'File' tab on page menu.
3. Click 'Paste JSON'.
4. In 'Swagger JSON' field paste content of json file available here.
5. Click 'Import' button.