TIER midPoint - Docker Reference Implementation

TIER Reference Implementations are designed to enable rapid evaluation of a component or set of interconnected components and provide a starting point for a full campus deployment. Reference Implementations are developed for Docker Swarm but dependencies are minimized within the containers in order to facilitate the use of other container orchestration mechanisms.

Introduction

Evolveum midPoint is a registry/provisioning tool selected as one of components of the TIER architecture. This document highlights packaging requirements for the component in the context of a Reference Implementation for production campus deployment. This approach simplifies the work needed by campus deployers, providing a fully functional service that can either be used as-is with additional campus support work or as

A production deployment of midPoint designed to support a large-scale campus typically consists of (a) a server to operate the application itself, (b) the application's database, (c) LDAP infrastructure, and (d) Rabbit MQ. Many other environments are possible. Of these elements, LDAP is typically the only component operated in high availability mode. midPoint itself is operated in standard availability mode. The midPoint database needs provisions for backups but not for high availability.

Like other primary TIER components, the Large Production TIER midPoint Reference Deployment utilizes Docker SWARM. Confidential configuration information (keys, passwords, etc.) will be managed with Swarm secrets.

1. Components
   The docker-compose recipe will include the following major components
   a. midPoint itself, using the existing Docker container (at least for now).
   b. MARIA DB as the database, utilizing the existing “TIER” MARIA DB container
      i. See also "Discussion" below
   c. LDAP, via the TIER OpenLDAP container
      i. includes midPoint and COmanage schema
      ii. optionally includes default data from training
   d. RabbitMQ for messaging
      i. Existing functionality - account import from minimum person registry demo code
      ii. Expansion over time
   e. Shibboleth Service Provider
      i. InCommon configuration
      ii. To protect the midPoint application
   f. Rabbit MQ Tracer Application
   g. Potentially, optionally,
      i. a wiki or some other demonstration component.
   h. Logging
      i. All logs will be written to stdout using the TIER container logging format

2. High Availability
   a. LDAP only
   b. The initial TIER distribution will not focus on this

3. Post Install - send the users to a URL with “what is next”.
   a. Demonstration topic(s)
   b. Links to training
   c. Use cases, etc.

4. Discussion - Demonstration/documentation
   a. Availability of mysql table that can be a data source (few hundred users)
   b. Availability of midPoint demo users in ldap
   c. Availability of midPoint demo roles / groups
   d. Yes - see above - Demo RabbitMQ subscriber that writes to a log file

      i. midPoint tied into the message bus – messages for a new creations, etc.

5. Software Updates
   a. See google notes document for now.