TIER COmanage - 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.

A production deployment of COmanage that is designed to support a large-scale virtual organization typically consists of (a) a web server to operate the application itself, (b) the application's database, (c) LDAP infrastructure, and (d) a SAML IdP/SP proxy. Many other environments are possible. Of these elements, LDAP and the SAML proxy are typically operated in high availability mode since they are usually directly involved with most authorization flows. COmanage itself is generally operated in standard availability mode since enrollment flows and organization management activities are not usually needed to be highly available. The database needs backups but not high availability.

1. Logistics
    a. Leverage the Docker container provided by the COmanage team
        i. https://github.com/Internet2/comanage-registry-docker
        ii. Includes
            1. Basic application on apache web server
            2. Shibboleth Service Provider
        iii. Note for initial build build: export COMANAGE_REGISTRY_VERSION=3.0.0-rc1
        iv. Pre-built containers in DockerHub - https://hub.docker.com/r/sphericalcowgroup/comanage-registry/https://hub.docker.com/r/sphericalcowgroup/comanage-registry-slapd/
            1. Initial version to use the Release Candidate versions: 3.0.0-rc1-shibboleth-sp/sphericalcowgroup/comanage-registry:3.0.0-rc1-shibboleth-sp
            2. Look at: https://github.com/Internet2/comanage-registry-docker/blob/master/docs/advanced-configuration.md for configuration options, examples, defaults, etc.
    b. Database – MARIA DB
        i. We use the “TIER” MARIA DB container.
        ii. This database is suitable for evaluation and prototyping purposes but no attempt has been made to configure it for production services.
    c. LDAP
        i. OpenLDAP
        ii. Either the TIER OpenLDAP or COmanage OpenLDAP container will work
        iii. The COmanage LDAP includes eduPerson and openssh-lpk.ldif (as does a version of the TIER LDAP)
    d. IdP/SP SAML Proxy
        i. SATOSA
    e. Logging
        i. All logs will be sent to stdout using the TIER container logging definition.
2. High Availability
    a. This would be typically implemented for the SAML proxy and LDAP only.
        i. OpenLDAP (master/slave)
        ii. Two SATOSA containers
    b. We do not presently implement high availability in Reference Implementations.
3. Post Install
    a. Users should view the COmanage documentation for initial steps after the startup of the system.
4. Configuration and demonstration tools provided in this implementation
    a. COmanage will use the LDAP provisioner
    b. Mediawiki will be bundled as a demonstration application through the SATOSA proxy