Rice University Project Plan

Executive Summary

Rice is interested in the Campus Success Program because of the advantages that moving to the TIER architecture can provide, standardization, modularization, and best practices. We are on the small side when it comes to staff and resources available to support our campus. Being able to leverage standard components will assist us as we try to move our infrastructure to something more scalable and efficient, allowing us to focus our efforts on the IdM issues the campus has instead of the IdM architecture itself.

Our current system was designed and developed 12 to 15 years ago. While it has had the flexibility to expand over time and as needs have changed, we have reached a point where further expansion is problematic. The system has reached a point where the complexity and tightly coupled nature of our IdM system means that changes in one area effect other areas in negative ways. Because of the small staff size of our IdM group, we don't have time to develop a new system from scratch that implements all of the best practices of a modern system.

Because of this, we have been eagerly awaiting the arrival of a TIER sanctioned entity registry and the definition of the integration pieces necessary to glue all of the components together. With the announcement of the decision to use the midPoint product by Evolveum as the reference entity registry and provisioning engine we feel that the time is right to move forward with rearchitecting our IdM system. We expect that fully replacing our existing system will take more time than the Campus Success Program will allow. But we will start down this road by setting up a testing environment using this component where we can gain familiarity with the product and have a place where we can build and implement the integration pieces necessary for our campus environment with the eventual goal being to switch over to it as our main production system.

We've been running Grouper and the Shibboleth IdP since 2009 and are currently running Grouper 2.2.2 and Shibboleth 3.3.2. Both components are utilizing our 389 Directory Server LDAP infrastructure, Grouper provisioning directly to it using PSP, and the Shibboleth IdP using it as it's authentication and attribute source.

Some of the difficulties that we've experienced trying to move toward the TIER packaged versions of these components are the need to run the old provisioner (PSP) with Grouper due to issues we have with PSPNG and needing to support the CAS protocol with our Shibboleth IdP, since it requires an external data source for session management. These issues mainly revolve around not understanding how to extend the packaged Docker components to make the changes we need in a way that allows us to fully utilize the new components in a high availability production environment.

We will be setting up the TIER packaged versions of both of these packages first in a test environment to get comfortable with and an understanding of what it will take to run these Docker components in production. For example: how to handle configuration, patching, maintenance and monitoring. Once we are comfortable with our ability to handle these tasks, we will move them into production.

Organization Description

Rice University, established in 1912, is a private (R1) research university located on a 295-acre campus in Houston, Texas. With a focus on undergraduate education, Rice maintains a student to faculty ratio of 6:1 with a median class size of 15. About 65% of undergraduates participate in research during their time at Rice. Rice has a population of 3879 undergraduate and 2861 graduate degree-seeking students along with 671 full-time and 210 part-time instructional faculty and around 2300 full and part-time staff. Rice offers degrees in the schools of Architecture, Business, Continuing Education, Engineering, Humanities, Music, Natural Sciences, and Social Sciences.

Containerized TIER Component(s) to be implemented

- Shibboleth IdP and SP
- Grouper Access Management Software
- Entity Registry, such as midPoint

Short Management-Level Use Case Description of Your Project

This project will be focusing on three areas:

- Building and documenting how we built a docker environment to run the components in a high availability, load balanced production environment
- Understanding and documenting how to customize the dockerized Grouper and Shibboleth components for our requirements
- Building and documenting a full TIER testbed to serve as the development point for further integration work.

Scope

- A non-production (NP) and production (P) docker environment that supports
    - High Availability (P)
    - Load Balancing (P)
    - Application Configuration management
    - Software Component upgrades
    - Logging (NP/P)
    - Monitoring (NP/P)
- Documentation of our build out of the DevOps environment covering the above topics for non-production and production
- The TIER packaged Grouper and Shibboleth IdP running in the production docker environment (We will not be implementing the Shibboleth SP at this time)
- Documentation of the component configuration changes needed to support Grouper and Shibboleth and the customization changes to add our needed functionality, CAS and PSP.
- A local TIER development testbed running within the non-production docker environment to be used for the redesign of our existing IdM functionality with:

- midPoint
- Grouper
- Shibboleth IdP
- RabbitMQ
- PostgreSQL Database
- 389 Directory Server

Key Stakeholders

Sponsor	Klara Jelinkova, Vice President for IT & Chief Information Officer
Campus Success Program Contact(s)	Dean Lane, Manager of Identity and Access Management, dlane@rice.edu
Communications contact	Liz Brigman, Senior Technical Writer & Editor
Project manager	Dean Lane, Manager of Identity and Access Management
Project team members	Dean Lane, Manager of Identity and Access Management Paul Engle, Systems Administrator III Brian Woods, Systems Administrator III
Deployment Partners/Contractors	N/A

Project Milestones

Activity	Assigned Resources	Start State	End Date
Design DevOps Environment	• Brian Woods • Dean Lane	2018-01-22	2018-02-16
Document & Diagram DevOps Design	• Brian Woods • Dean Lane	2018-02-09	2018-03-09
Build DevOps Environment	• Brian Woods	2018-03-12	2018-05-04
Revisit DevOps Documentation with Lessons Learned	• Brian Woods	2018-05-14	2018-05-18
Build out Non-Production Standalone Components - DB, LDAP	• Dean Lane	2018-03-12	2018-03-30
Update Shibboleth to use CAS, DB and LDAP servers	• Paul Engle	2018-02-12	2018-03-09
Document Shibboleth configuration changes above base	• Paul Engle	2018-03-12	2018-03-23
Update Grouper to use to use PSP, DB and LDAP servers	• Paul Engle	2018-03-26	2018-04-20
Document Grouper configuration changes above base	• Paul Engle	2018-04-23	2018-05-04
Test Shibboleth & Grouper in Non-Production environment	• Paul Engle	2018-05-14	2018-05-25
Test Shibboleth & Grouper in Production environment	• Brian Woods • Paul Engle	2018-05-28	2018-06-08
Update midPoint to use DB and LDAP servers	• Dean Lane	2018-04-02	2018-04-27

Document midPoint configuration changes above base	• Dean Lane	2018-04-30	2018-04-04
Test midPoint in Non-Production environment	• Dean Lane	2018-05-14	2018-05-25

Synergistic Projects

N/A

Constraints, Assumptions, Risks and Dependencies

Constraints	That virtual hardware will be available for all of the systems that will need to be stood up to support this architecture.
Assumptions	That individuals with more extensive Docker experience will be available to answer questions and vet solutions. That individuals with knowledge of the Grouper and Shibboleth Docker configuration points will be available to answer questions.
Risks and Dependencies	That something in our existing infrastructure or processes breaks and must be fixed taking time away from the project. Vacations may slide the schedule a bit.