University of Maryland Baltimore County Project Plan

Executive Summary

UMBC has been involved in supporting and advancing middleware and identity management since the year 2000, when we were one of ten universities selected to be part of the Internet2 Early Adopter program.

For UMBC, the early adopter program was transformative in that is demonstrated the importance of identity management. UMBC has invested and used identity management as key component of our institutional technology strategy. UMBC was one of the first fifty universities as members of InCommon, one of the first universities to participate in the Certificate program, one of the five universities to go through the InCommon assurance program, one of the early adopters of Duo, and more recently one of the early investors in TIER. At UMBC, we believe in the power of community, and we feel that TIER is essential to advancing the InCommon community.

Our goals for joining this program are to threefold: First, UMBC would like to migrate our mature Shibboleth infrastructure to make use of the TIER deployment model. Second, we believe in Grouper and intend to make Grouper a core component of our group access control strategy. We will do this by implementing Grouper using the TIER containers. Along with that effort we will replicate, via Grouper, our campus portal groups into Google groups. Third, we designed our identity infrastructure without an intermediary identity registry. We are very interested in moving to midPoint and revamping our identity architecture. Our proof-of-concept will be to roll out midPoint for the management of our adhoc guest accounts.

Organization Description

UMBC is a mid-sized public research university located just outside of Baltimore and 30 minutes north of Washington, DC. UMBC emphasizes science, engineering, information technology, human services and public policy at the graduate level. Our student body is comprised of 12,000 undergraduate students and 3,000 graduate students.

Containerized TIER Component(s) to be implemented

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

Key Stakeholders:

Sponsor	Jack Suess, VP and CIO
Communications Contact	Jack Suess, VP and CIO
Project Manager	Todd Haddaway, Director
Project Team Members	Paul Riddle (Shibboleth), Jason Griego (Identity Registry), Chris Sutherin (Grouper)

Grouper

Use Cases:

I. Make use of the TIER Grouper Docker environment for installation and upgrades

- Migrate from a manually installed and configured Grouper environment to use the TIER Grouper release. The result of the automated install needs to use our back-end Oracle database.

II. Auto-provision Google groups based on Grouper group membership

- Create Google groups based on course enrollment, as well as Google group membership based on membership in one of our campus portal groups. Clubs and organization now using our campus portal groups would have an auto-provisioned Google group.

Project Milestones:

Activity	Assigned Resources	Start State	End Date
Determine best TIER solution for us. AWS image, OVA or Docker image	Chris, Todd	10/23/2017	10/30/2017

Stand up test environment based on TIER delivery option selected	Chris	10/30/2017	11/17/2017
Configure Grouper to use Oracle database	Chris	11/20/2107	12/18/2018
Configure Grouper with UMBC customizations.	Chris	12/18/2017	1/15/2018
Test initial setup	Chris, Todd	1/15/2018	1/29/2018
Determine if multiple Grouper TIER environments should be used for UI, loader and web services	Chris	1/29/2018	2/5/2018
Work with myUMBC staff to determine the list of groups to be auto provisioned into Grouper	Chris, Todd, Collier, Jack	1/29/2018	2/12/2018
Configure Grouper to load myUMBC groups	Chris	2/12/2018	3/18/2018
Test myUMBC groups load	Chris, Todd, Collier	3/18/2018	3/26/2018
Configure Grouper to provision myUMBC groups to Google	Chris	3/26/2018	4/23/2018
Test complete system	Chris, Todd, Collier	4/23/2018	5/25/2018
Training	Chris, Todd, Collier	5/26/2018	6/15/2018

Constraints, Assumptions, Risks and Dependencies:

Constraints	Time of the individuals necessary to accomplish these tasks.
Assumptions	That there is an appropriate communication method with myUMBC such as Amazon messaging. That Grouper will allow the customizations necessary for UMBC specific requirements such as using Oracle as a database
Risks and Dependencies	Not being able to communicate effectively and efficiently with myUMBC

midPoint

Use Case:

Guest account provisioning

UMBC's current IDMS system was created in the early 2000s. While it's functionality is robust, the technology on which it is built has aged. Most scripts are written in Perl and until recently, we made use of Netscape iPlanet / Sun JavaOne for directory

services. Port389 is now used. Domain and script knowledge is known by one staff member. It is critical that we move to a more modern and standardized platform. If midPoint is TIER's solution for this problem, we would like to work to migrate from our legacy system to midPoint. The starting point / proof-of-concept project for UMBC would be a guest account system. We have a need to be able to easily provision accounts for guests, both in bulk as well as individuals. An example would be "I have a group of 30 people coming in for a two-day seminar that will need to authenticate to lab computers." Or "I am a guest library patron for the day and need to be able to use online library resources." Long term, we are looking to replace our current home-grown IDM with an open source solution such as midPoint.

Scope

This project will be replacing the existing facility for bulk temporary accounts ("ceduc accounts") as well as creating a new facility for very short term temporary accounts. Containerized midPoint will be released in a high-availability configuration with an Oracle database backend. Existing user registry information will be synchronized from IDMS. If needed, an external user interface will be created to supplement midPoint UI for requesting accounts; this would be backed directly by midPoint to the greatest extent possible.

Project Milestones:

Activity	Assigned Resources	Start State	End Date
Create design documents and diagrams	Jason, Todd	10/16/2017	10/27/2017
Deploy containerized midPoint backed by Oracle	Jason, Chris, Todd	10/30/2017	11/17/2017
Configure containerized midPoint to be highly-available (optional)	Jason	11/27/2017	12/8/2017
Synchronize person and account information with IDMS	Jason	11/27/2017	12/22/2017
Create Guest Account request & management user interface	Jason, Todd, Collier	1/2/2017	2/23/2017
Create Guest Account request & management testing framework	Jason	1/2/2017	2/23/2017

Create midPoint account status data push to IDMS	Jason	1/2/2017	2/23/2017
Create midPoint approval workflow	Jason	2/26/2017	3/23/2017
Document guest account request and maintenance process (user, approver, and TSC targets)	Jason, Todd	3/26/2017	4/6/2017
Production release	Jason	4/9/2017	4/13/2017

Constraints, Assumptions, Risks and Dependencies:

Constraints	Time of the individuals necessary to accomplish these tasks.
Assumptions	Containerized midPoint will be available in Fall 2017. midPoint training will be available.
Risks and Dependencies	Minimal.

Shibboleth:

Use Case:

Make use of the TIER Shibboleth IdP Docker environment for installation and upgrades

UMBC has a mature Shibboleth IdP environment. Currently, we are running Shibboleth v3.3. While most SPs that we deal with are Shibboleth based, using the v3.3 feature, we now have CAS integrations as well. UMBC would like to migrate our Shibboleth infrastructure to make use of the TIER deployment model. Currently, we do not have a good model for keeping configurations in sync between our three nodes. It’s a manual process, and cumbersome to maintain. TIER should make all of that much easier. We feel that this will be a beneficial project to the Campus Success Program in that it will show a migration path for existing Shibboleth installations and the advantages that TIER brings.

Project Milestones:

Activity	Assigned Resources	Start Date	End Date
Choose platform for TIER instance of Shib Idp; to be load-balanced with existing non-TIER instances initially (leaning towards AMI)	Paul	10/23/2017	10/30/2017
Install and test vanilla Shibboleth IdP on new TIER instance	Paul	10/30/2017	11/17/2017
Clone IdP configuration from current production (non-TIER) Shibboleth IdP instances	Paul	11/17/2017	12/18/2017
Figure out the best way to integrate TIER Shib with UMBC’s legacy SSO system that currently handles all of our AuthN	Paul	12/18/2017	1/15/2018
Limited production test of new TIER instance (via /etc/hosts or similar method)	Paul, Todd	1/15/2018	1/31/2018
Place TIER instance in active load-balancer rotation with current production instances	Paul	1/31/2018	2/28/2018
Decide on configuration for production TIER-based Shibboleth IdP deployment, using both on-site (VM) and off-site (AWS) resources	Paul	2/28/2018	3/31/2018
Setup and configure production TIER deployment (possibly making use of existing IdP VMs)	Paul	3/31/2018	5/31/2018
Switch production IdP to be 100% TIER-based deployment	Paul	5/31/2018	6/30/2018

Constraints, Assumptions, Risks and Dependencies:

Constraints	Available staff time; getting up to speed with the new platform
Assumptions	TIER Shib instance will be flexible enough to accommodate UMBC’s fairly extensive custom IdP business logic (intercept flows, etc)
Risks and Dependencies	Issues getting legacy SSO platform up and running in TIER-based environment