CAS, Shibboleth,
And an evolving SSO approach

Prepared by Joe Fischetti
Linux System Administrator
Information Technology
February 27, 2017

#NERCOMPIdM
Topics

- Marist Background
- About the presenter
- Marist Identity environment
- Marist Single Sign On
- Shibboleth HA
- Marist Email
- IDM/SSO Implementation Notes
Marist College is...

- Comprehensive liberal arts institution
- “is noted for its leadership in the use of technology to enhance the teaching and learning process.”
- Founded in 1929
- Overlooks the Hudson River
- Around 7000 students
- 2000 Faculty/Staff (including adjunct)
- Close relationship with IBM
  - LinuxOne Community Cloud
About me

- **Name:** Joe Fischetti
- **10 years as a systems integrator in the residential AV industry**
- **Started at Marist in April 2017**
- **Tech interests:** Crypto, security, system scalability
- **A.S. Information Science and Technology**
- **B.S. Computer Science**
- **Enjoy programming:** Java/PHP/Bash
- **Responsibilities at Marist include:**
  - Apache VCL
  - Shibboleth
  - Linux Lab
  - VMWare/ESX infrastructure
  - Load balancers
Abbreviations in presentation

- CAS [protocol] - Central Authentication Service
- IdP - Identity Provider
- SAML - Security Assertion Markup Language
- SLO - single logout
- SP - Service Provider
- SSO - single sign on
- XML - eXtensible markup language
Marist Identity Environment

- **Banner**
  - System of record for Marist Persons

- **LDAP**
  - System of record for Marist accounts

- **Active Directory**
  - Used for windows and mac logins
  - Small subset of all our users
Banner Enterprise Resource Planning (ERP)

- Oracle databases on zSystem
- Faculty, Staff, Administrators, and Students all have records in Banner
- Admissions, Registrar, Student financial services input information
- Self Service Banner is available via portal
LDAP

- 4 AIX servers
- IBM Tivoli Directory Service
- Main source of user/course information
- Banner persons plus:
  - VENDOR
  - AFFIL
  - ALUM
  - GUEST
- Feeds out to card swipe, marist money, AD, etc.
Active Directory

- 3 domain controllers
- Used for Windows and Mac authentication
- Relatively small subset of the whole environment
  - 1800 users
  - 500 groups
  - 1800 computers/servers
- Password sync with PGP on windows laptops
- Group policy for Windows management
- Azure AD - Office 365 environment
  - Synchs from LDAP, not on prem AD
Syncing

- Users are fed into Banner by Admissions, Registrar, Student financial services.
- Banner feeds run 6 times per day
  - Push changes to LDAP servers
- Changes in LDAP are pulled to AD and Azure (separate processes)
Marist Persons

Windows PC

MAC

Active Directory

Admin Department

LDAP

Banner ERP

E-mail

Card Access

Marist Money

Shibboleth

CAS

Shibboleth

CAS

Marist Money

Card Access

E-mail
Single Sign On
SSO General

- Desired Ux - User experience.
  - User should only have to enter their password ONCE to access all the resources they need
    - Not **required**, a goal
  - Centralized:
    - Management - passwords are managed in one place
    - Authorization - Users can be granted/denied access to a number of endpoints from one place.
Side effects of SSO

- One password lost means access to everything
- Difficult
  - Coding
  - Getting systems to work together
  - Support
1. User requests web page from SP  
2. SP responds with a redirect to the IdP, includes a SAML statement for the IdP to identify the SP  
3. User's browser requests log in page from the idp (with SAML from SP)  
4. IDP checks for session cookie, if not, IDP provides authentication (most often, user provided password)  
5. IDP creates a session cookie for the user, and sends redirect back to user's browser including the SAML assertion  
6. User's browser POSTs the provided SAML assertion to the SP.  
7. SP verifies the assertion, extracts attributes  
8. User good to go

Two paths of communication (User ↔ SP, User ↔ IdP)
SAML Flow - continued

Redirect to Shibboleth for authentication

SAML Assertion

SAML Assertion

Marist Mail

Shibboleth IDP
SAML Flow - continued...

- Subsequent visits to other SP's will bypass step 4
  - This means the user doesn't need to enter their password again
- Subsequent visits to an already active SP will typically bypass the entire flow (steps 2-7), due to valid session cookies with the SP
  - This means the user doesn't need to enter their password again
  - It also means that if rights have been revoked [at the central location].... user still has access to the sp.
  - “Remember Me”
SAML Configuration

- SAML2 is... more software
  - SP runs along side web applications, behind apache.
  - Apache gets request for protected resource... SP handles it... then passes information to the application.
CAS protocol

- CAS doesn't pass data in SAML assertions [through the user's browser]
  - Direct communication between the Service and the IDP
- Authenticated user gets a ticket, provides that ticket to the service, and the service uses that ticket to get info from the IdP
- There's 3 paths of communication.
  - (User ↔ Service, User ↔ Server, Service ↔ Server)
- No "SP" software. The application is the service.
  - Don't want to use apache? Don't have to.
CAS Flow

Redirect to CAS for authentication

Ticket -> Marist Mail
Ticket -> User info
Ticket -> Shibboleth IDP

Validate Ticket

User Attributes
1. SAML assertion is passing through the user... can't the user manipulate the data?
   a. Not necessarily... SAML assertions are (optionally) signed/encrypted between the idp and the SP. Encrypted data isn’t visible in the clear to the user.

2. If a service provider uses an (unrealistically long) life for it's session...
   a. Changes made to the management server won't have an effect for a while
   b. Example:
      i. User signs in to mail with an 18 hour session lifetime
      ii. User password changed, but email session is never ended
      iii. Email continues to work until next refresh

3. Not a browser problem... Some apps do this
Marist SSO

- The original Shibboleth configuration:
  - idp.it - shibboleth server for webex, listening on 8443
  - idpv3.it - shibboleth server for marist mail pilot. “New IdP”
- CAS - apareo CAS server for ilearn/mymarist/etc. etc. etc.
- ldap - Foxmail/2, plus direct authentication for various internal services
- No shared SSO for webex, new marist mail, and just about every other marist service
  - Management required in a number of different places
  - InCommon had us listed with idp.it, wouldn't let us update with idpv3.it
  - They don't want versioning in the entity ID
Marist SSO

- Completely new Shibboleth deployment:
  - Auth.it - shibboleth server for Marist Mail, Webex, 6-7 other SPs (and growing)
- Still have CAS/LDAP direct...
- CAS/Shibboleth are disjoint
  - One set of credentials, entered too many times
- Numbers:
  - CAS - 400k logins / month (Sept '17)
  - Shibboleth - 250k logins / month (Sept '17)
SSO Options

1. Shibboleth can do CAS protocol.
2. Shibboleth can act as the delegated authentication service for Apareo CAS.
3. Apareo CAS could be SAML IdP.
4. Abandon CAS completely
SSO Options - Drill down

● Shibboleth can do CAS protocol.
  ○ Services **might** require a rewrite and IdP requires additional configuration.
  ○ Added complexity to Shibboleth.

■ Documentation is key
SSO Options - Drill down

- Shibboleth can act as the delegated authentication service for Apareo CAS.
  - Services don't (shouldn’t) need to be modified.
  - IdP needs to see CAS as an SP.
SSO Options - Drill down

- Apareo CAS could be SAML IdP.
  - No point, too far into Shibboleth.
  - OTOH, CAS is already down level, needs to be updated.
SSO Options - Drill down

- Abandon CAS completely
  - Force applications to move to Shibboleth/SAML2.
  - Some applications require extensive work to enable SP support.
SSO Options

1. Shibboleth can do CAS protocol.
2. Shibboleth can act as the delegated authentication service
3. Apareo CAS could be SAML IdP
4. Abandon CAS completely
Shibboleth HA
Incredibly important for everybody
  ○ Students (customers) need access to services all the time.

Services should be available even during maintenance
  ○ Internal shift from “Server = Down” to “Service = Down”
  ○ Just because a server is down [for any reason] doesn’t necessarily mean customers are affected.
  ○ [big public service].com is always available, why can’t we be?
High Availability

- Shibboleth IDPs should handle logins
- Persistent Sessions aren’t critical
  - If we fail over, users can log in again
  - One server can handle load without a problem
  - Adds to simplicity
- Cluster consists of 3 separate [nearly] identical servers.
Load Balancing

- Requires a DNS change
  - auth.it.marist.edu CNAME auth.it.ha.marist.edu
- Load balancers (LB)
  - handle all requests for *.ha.marist.edu
- Server Load Balancing (SLB)
  - Two local servers with proxy type access through the LB
- Global SLB (GSLB)
  - Different DNS response for an off-site server
GSLB IP Address

GSLB IP = VIP OR Offsite IdP

Virtual IP

Primary IdP

Backup IdP

Offsite IdP

GSLB Zone

DNS Server

service.marist.edu

service.ha.marist.edu

“A10”
Marist Email
Email

- Email for life
- 5 different email systems
  - IMAP and IMAP2
  - IBM Notes on prem and in the cloud
  - Office 365
- Every user still has @marist.edu
Email

● IMAP and IMAP2
  ○ @mail.marist.edu
  ○ Older software versions
  ○ Older web interface
  ○ Small mailboxes
  ○ Over capacity (needed to create a new server)
IBM Notes on prem and in the cloud
  ○ @notes.marist.edu
  ○ On prem existed first, then started moving users to the cloud
  ○ Notes server knows which mailbox to deliver mail to.
Email

- **Office 365**
  - @o365.marist.edu
  - Newer initiative
  - Many users are already used to the office suite
  - Exchange is widely supported
Idm/SSO Implementation Notes
Mixture of standard and custom user attributes

- maristcwid - unique, immutable
  - eppn = maristcwid@marist.edu
- maristpwwarning - password expiration
- mailpreferenceoption - mail forwarding info
- maristmailpref - marist email address

- mail
  - multiple values
  - mary.marist@marist.edu
  - mary.marist1@marist.edu
Our password policy:
○ Passwords do expire for fac/staff
○ expiration has a 15 day notification period
○ expiration notification is emailed, and presented to the user at login-in
○ Flag in LDAP is used to get password status
  ■ -1, 0, 1
● Shibboleth custom flows handle the password expiration field
Logout

- How does logout work with Shibboleth?
  - ‘It doesn't'
- Service providers store their own session cookie
  - Logging out at the IdP doesn't log you out of each service provider.
- Shibboleth SLO does exist
  - Log out page in IDP logs the user out of the idp then loads a page with the logout url of all SP's that were connected.
  - Considered a “best-effort” attempt.
- Our practice, with internal SPs
  - Load their local logout link, with a redirect to the idp logout
  - Still doesn't log user off of OTHER SP's. But new SP’s won't get on.
Inventory

- **CAS** - "allow all services from [https://*.marist.edu](https://*.marist.edu)"
  - Any service can get on without changing the server config....
  - No way to identify what's been leveraging it without running an audit on the logs.
  - Wouldn't help with seasonal application usage.
- **Shibboleth** solves this (in part) with the metadata requirement.
  - Still part of a federation, so anything in InCommon can use it.
  - Wildcarding the service URLs is fast and easy.
Helpful Links/Resources:

- [https://www.marist.edu](https://www.marist.edu)
- [https://wiki.shibboleth.net/](https://wiki.shibboleth.net/)
- [https://www.shibboleth.net/community/lists/](https://www.shibboleth.net/community/lists/)
- [https://linuxone20.cloud.marist.edu/cloud/](https://linuxone20.cloud.marist.edu/cloud/)
Questions?