Stranger Things:

An Academic Sierra Inn Reach Library moving to Innovate AWS

Tuesday, May 7, 2019

3:00 - 4:00 LAVEEN M05

Draft Slide Deck 05/01/2019

Outline

- Project Background
- Campus Partners
- Software Only / Hosted evaluation
- License negotiation
- Implementation
- Innovative Single Sign On
- Implentation / Go Live
- Post Go Live
- Inn Reach SSO
- Miscelaneous
- Things I'd have done differently

Outline

- Project Background
- How we decided on hosted
- Implications of hosted and SSO
- Getting to the signed contract
- Implementation project
- SSO configuration & testing
- Go Live
- Post Go Live
- Interesting tidbits
- Things I'd have done differently

Project Background

- BGSU was a founding member of OhioLINK which was the first Inn Reach sites in 1992
- Our Inn Reach Partners:
  - OhioLINK (Academic Library Consortia in the State of Ohio)
  - SearchOhio (Public Library Consortia in the State of Ohio

17% of all our initial circulations at BGSU are Inn Reach (excluding reserve/equipment/closed stacks)

Project Background

- BGSU UL Innovac implementation -1992
  - Turnkey server customer
  - maurice.bgsu.edu
- BGSU UL migrated to Millennium - 2004
- Implemented WAM fro remote access – 2005, migrated to Eproxy in 2014
- BGSU implemented LDAP for patron login (My Library Account and WAM) -2009
- BGSU UL Summon Discovery Layer -Spring 2011
  (Encore Discovery Layer would require additional III AWS server)
- BGSU UL migrated to Sierra - 2013
  Sierra required two server's:
  - maurice.bgsu.edu application server we purchased - 2010
  - sierra-db.bgsu.edu database server we purchased - 2013
- AWS implementation Jan - 2018

Project Background

- In 2015 started thinking about server replacement.
  - Current Sierra application server was a six year 32 bit OS application server
  - Age of server left us with no Sierra migration path due to 2.1.0_4 and beyond have a 64 bit OS server requirement

- In the June of 2016 our turnkey application hard disk array die.
  - Innovative fixed it and got us back up and running.
  - They rebuilt the disk array with 64 bit software so we were able migrate up to Sierra 3.1.3

- Fall 2016 Central IT had project to get all servers out of old server room by Jan 2017

- Fall of 2016 BGSU Chief Information Officer indicated that central IT could virtualize two servers we would need for Sierra

Campus Partner

- BGSU Central IT - software only evaluation (Jan – March)
  - Meetings with BGSU ITS staff and III technicians
- BGSU Central Purchasing (May – July 2017)
  - Had to straighten out previous contract proposals
- BGSU Legal Office (June – September 2017)
  - Innovative wanted to replace the old file folder of purchase contracts between BGSU and Innovative
- BGSU Central IT / Library / Innovative Implementation (October 2017– Jan 2018)

Central IT / Virtual Machine evaluation

– Conference calls between BGSU Central IT and software engineers and managers at Innovative

(Dec 2016 – February 2017)

– Innovative requirements virtual machine servers:
  - root account
  - iii root account
  - 24/7 access to the virtual server.

  These 3 requirements where problematic from my Central IT security standpoint.

– Central IT asked for a spec document regarding which software release libraries were using so they would know what security patches to install on server or not to install without bringing down Sierra software. Innovative did not have such documentation at that time.

– Virtual machine install process: Innovative Sierra software for server's is installed by a technician via self extracting software loads on a virtualized server. My central IT could watch the process but could not veto any libraries they might identified as a security risk.

Central IT / Hosted evaluation

- Evaluate the hosting landscape:
  - With our turnkey server located in a BGSU server room we used LDAP for My Library Account and WAM authentication
  - Central IT security protocols no longer allowed the use of LDAP for off-campus third party software applications.
  - III AWS hosting require us to annually license Innovative SSO software for using campus credentials. SSO requires another server for Apache process.
  - BGSU Central IT sent a security questionnaire to Innovative Cloud Operations

    5/17 - BGSU Security staff impressed at Innovative responses.

Central IT / Hosted evaluation

Innovative hosting costs negotiations started

- Dennis Carter our Sales Representative
- Worked out details in May of 2018
- 3 servers needed in AWS cloud:
  - Application server — sierra-app.bgsu.edu — Sierra Client
  - Database server — bowlg-db.iii.com — SQL pgAmin access
  - SSO server — maurice.bgsu.edu — Apache Server

  - BGSU has 1.2 million Bibliographic records
  - As such we were classified by Innovative as a very large sized library for the virtualized server spec's that we would need for AWS hosting

Central IT / Hosted evaluation

Questions?

License Negotiation

- New Contract Documents (BGSU Legal with III Legal)
- **Bowling Green State University__Master Subscription License Agreement**
  - BGSU is an institution of the State of Ohio so contract resolution has to be in Ohio courts jurisdiction
- **Bowling Green State University__Perpetual License Agreement**
  - Identify software from past purchase to be identified and included
  - Remember to get odd little things like Millennium upgrade and the number of simultaneous staff logins we negotiated at that time
- **Bowling Green State University__ Professional Services Agreement**
  - cloud migration one time expenses
    - Sierra Application Server, Sierra Database Server
    - Sierra SSO server setup/sconfiguration

License Negotiation

- **Bowling Green State University__Master Subscription License Agreement**

INNOVATIVE INTERFACES INCORPORATED
SUBSCRIPTION LICENSE AGREEMENT

This Subscription License Agreement ("License Agreement") is entered into by and between Innovative Interfaces Incorporated, a California corporation ("Innovative"), and the party identified as Client below ("Client"), as of the "Effective Date" also set forth below.

Client	
Address	
Customer No.	
Effective Date	

1. **Definitions**.

"Authorized Users" mean Client's worldwide employees, third-party auditors, agents and contractors, as well as those users and employees operating in Client's member locations.

License Negotiation

- **Bowling Green State University__Perpetual License Agreement**
  - Identify software from past purchase to be identified and included
  - Remember to get odd little things like Millennium upgrade and the number of simultaneous staff logins we negotiated at that time

INNOVATIVE INTERFACES INCORPORATED
PERPETUAL LICENSE AGREEMENT

This Perpetual License Agreement is entered into by and between Innovative Interfaces Incorporated, a California corporation ("Innovative"), and the party identified as Client below ("Client"), as of the "Effective Date" also set forth below.

Client	
Address	
Effective Date	
Customer No.	

1. **Definitions**.

"Authorized Users" mean Client's worldwide employees, third-party auditors, agents and contractors, as well as those users and employees operating in Client's member locations.

License Negotiation

- **Bowling Green State University__ Professional Services Agreement**
  - cloud migration one time expenses
    - Sierra Application Server, Sierra Database Server
    - Sierra SSO server setup/sconfiguration

INNOVATIVE INTERFACES GLOBAL LIMITED
MASTER PROFESSIONAL SERVICES AGREEMENT

This Master Professional Services Agreement ("Services Agreement") is entered into by and between Innovative Interfaces Incorporated., a California corporation ("Innovative"), and the party identified as Client below ("Client"), as of the "Effective Date" also set forth below.

Client	
Address	
Customer No.	
Effective Date	

1. **Definitions**.

a. "SOW" means one or more Statements of Work executed by the parties hereto from time to time on or after the Effective Date, and attached to and made part of this Agreement as Exhibit A.

License Negotiation / Signed Contract

- Jim Tillman visited our site and gave a state of the company update at an all staff meeting. 9/21/17
- Had a meeting with the Dean afterward where all the final contract details finally worked out in the following week.
- Jim Tillman scheduled to visit the Ohio IUG Regional Conference in Columbus on 9/22/17
- Required my Dean and BGSU legal consul signatures at BGSU, as well as expense approval higher up, and CIO approval.
- Final contract signed by all parties Oct. 12, 2017

Implementation

- Communications: migrations@iii.com

- Innovative AWS hosted survey for implementation
- https://csdirect.iii.com/documentation/hosted_systems.php#related

- Innovative SSO survey for implementation
- https://techdocs.iii.com/iii_techdoc_sso.php
- SSO Integration Prerequisite From

Implementation

- Kick Off meeting questions from BGSU ITS
- What needs to occur before the environment will be available?
- When will the environment be available?
- How much time is needed for testing:
  - Application Server — sierra-app.bgsu.edu
  - Database Server — sierra-db.bgsu.edu
  - SSO/SLO server — maurice-test.bgsu.edu
  - BGSU SSO — testsso.bgsu.edu
  - Portlet — mytest.bgsu.edu
  - Firewall — campus and AWS
  - PeopleSoft test FTP server — daily patron load via iii scheduler product
  - Whitelisting email's from cloud server in BGSU email system
  - Inn Reach testing not available prior to Go-Live

Implementation

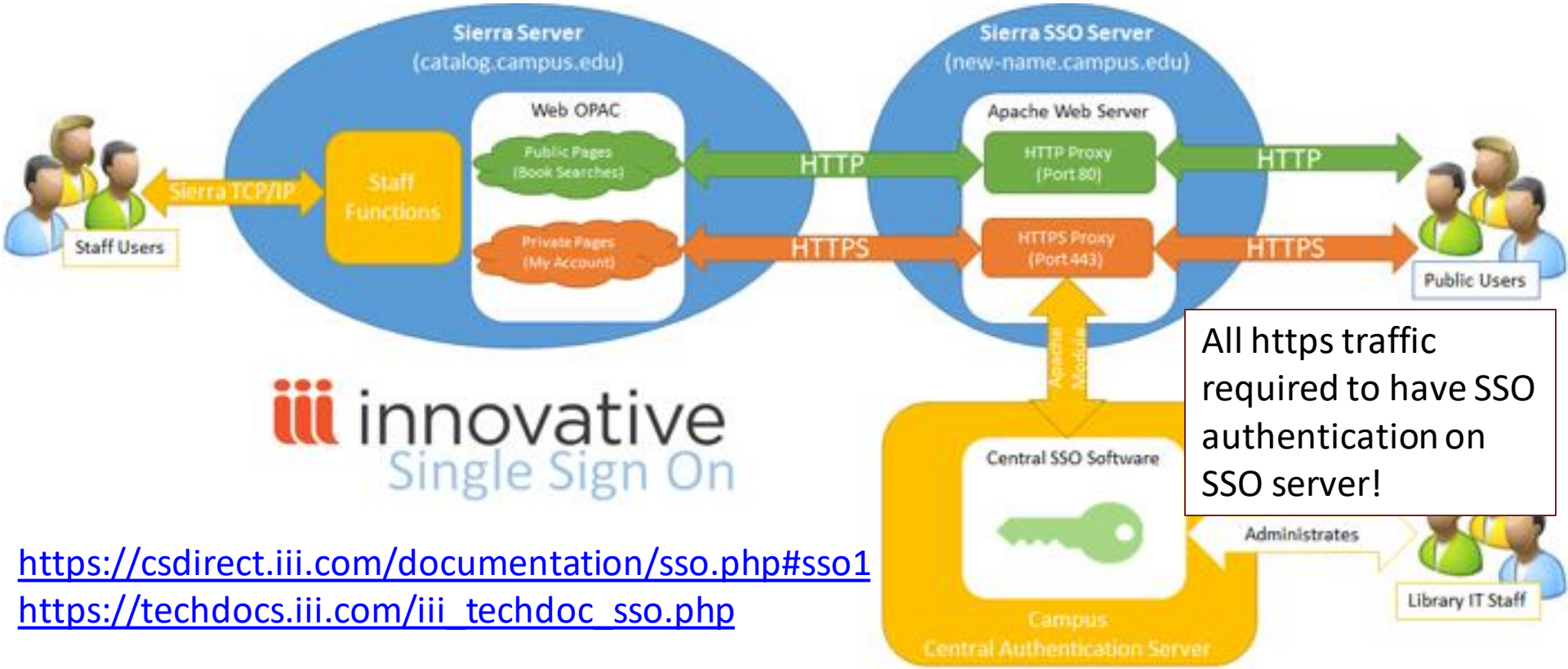
- 11/07/17 Kick Off Meeting Library/ITS & Innovative
  - BGSU ITS emphasize need for SSO test environment
  - (Not a normal part of AWS implementation with III at the time)
- 11/13/17 Innovative Cloud Opps created SSO test server
  - SSO server environment maurice-test.bgsu.edu
- 11/15/17 Innovative setup Sierra server's in cloud
    - Took data from our turnkey production to create test environment
    - sierra-app.bgsu.edu => bowlg.iii.com
    - sierra-db.bgsu.edu => bowlg-db.iii.com

Implementation / Single Sign On

- Single Sign On Server testing

- Innovative decided to setup a test SSO environment for utilizing the new hosted VM's that CloudOps. Used the data from our current Sierra environment and had to set up a new temporary valid FQDN, as well as an SSL cert to implement this environment.

Innovative Single Sign On



All https traffic required to have SSO authentication on SSO server!

https://csdirect.iii.com/documentation/sso.php#sso1
https://techdocs.iii.com/iii_techdoc_sso.php

Innovative Single Sign On

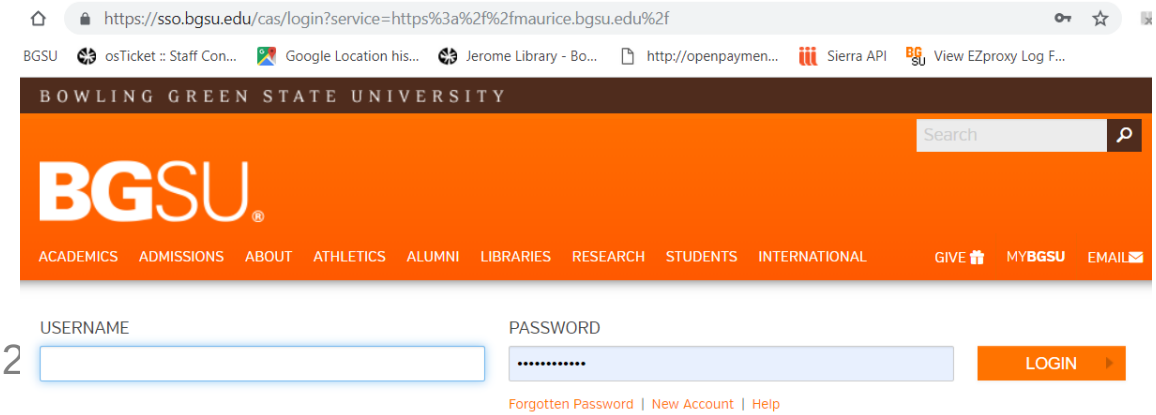
- Originally maurice.bgsu.edu was our application server name and I wanted to preserve all the bookmarks so I thought moving this to the SSO server name was the best path. Especially for old url's using Innovative WAM. (We migrated to Ezproxy as our primary off-campus electronic resource access solution, however we kept WAM as a backup access point.)

- Central IT chose to program our SSO setup using CAS architecture instead of Shibboleth (could have done either) based upon the Innovative response that they had expertise in both for SSO

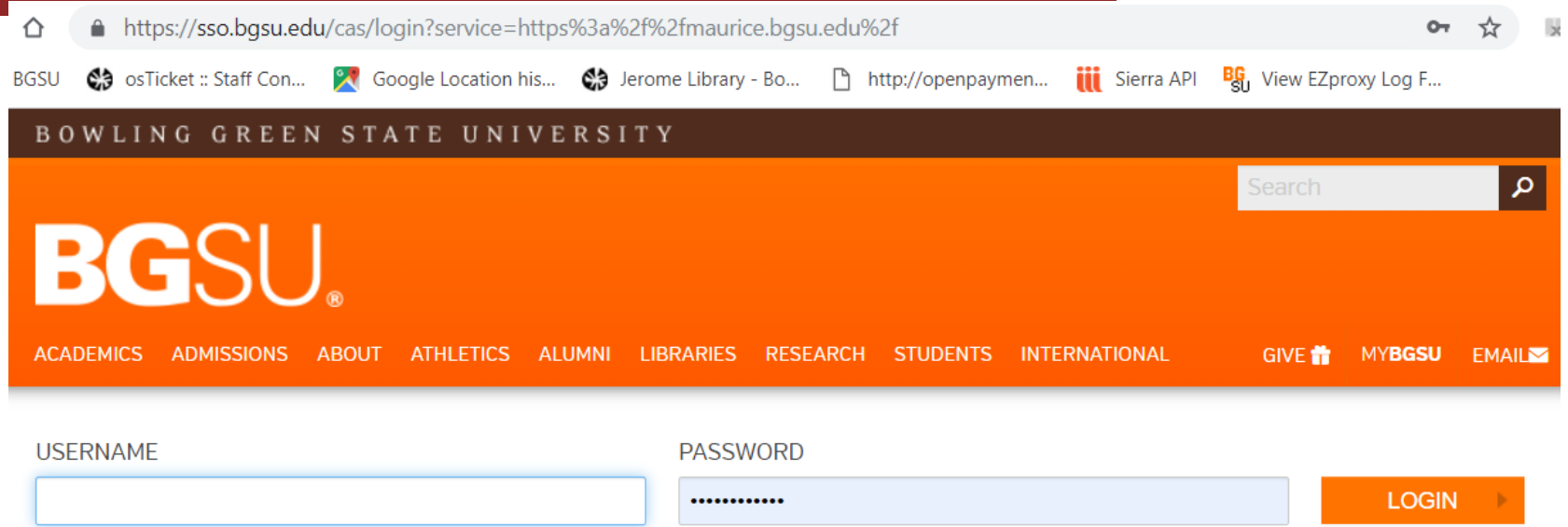
Innovative Single Sign On

What does it meant that All https traffic on SSO server is required to have authentication? It means that general public users of your webopac and campus users of your webpac have to be directed to different urls.

We use insecure page links from our Library home page so that campus affiliated and non campus users can search our catalog without login in. https://maurice.bgsu.edu redirects: to campus SSO login page:



Innovative Single Sign On



BGSU Central IT will not make us a separate login screen for the ILS SSO screen so https://maurice.bgsu.edu will be redirected to your campus single sign on screen first! So we have no way of redirecting our courtesy card holders back to the login url they will need to use.

Innovative Single Sign On

Currently BGSU uses insecure page links from our Library home page so that campus affiliated and non campus affiliated users can search our catalog without loging in. http://maurice.bgsu.edu

We want a single url to work for old bookmarks, campus SSO users, and community users so we have to use non https pages

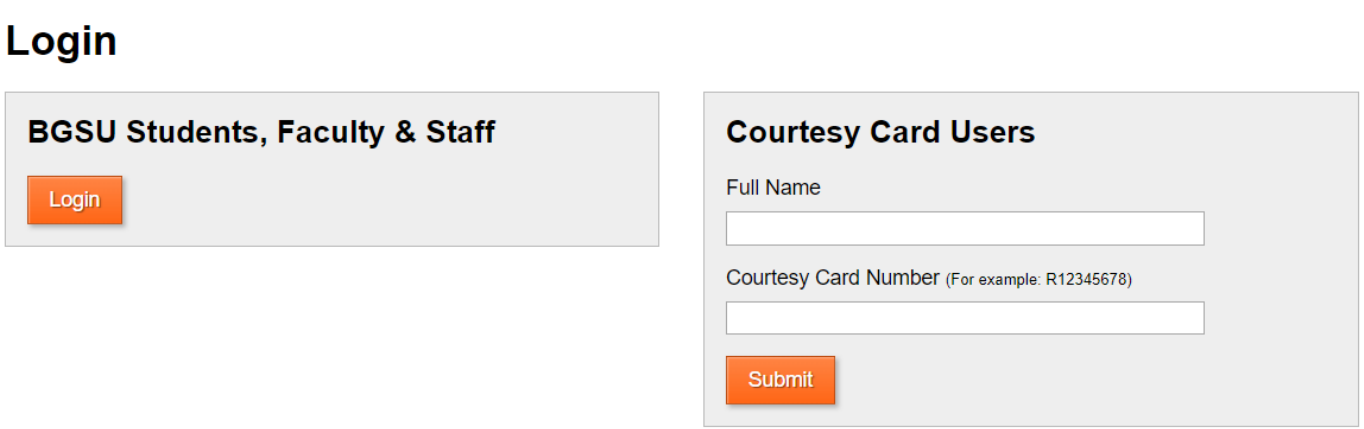
Innovative SSO Community User

- To log into the library account our web pages offer users the login screen for our sso server which is encrypted and that sends them to the campus single sign on screen.

- Our courtesy card holders can not log in this way. On a separate web page for their services we direct them to loggin to are application server
- https://sierra-app.bgsu.edu/patroninfo.html which does not have SSO.

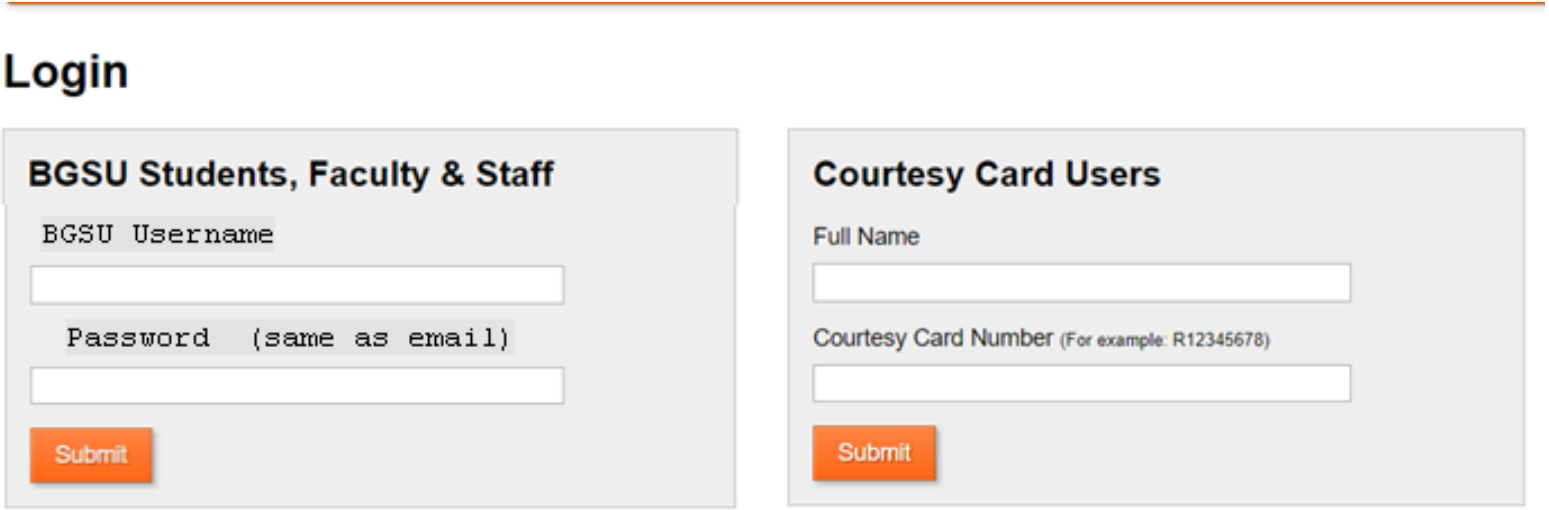
Innovative SSO Community User

- https://sierra-app.bgsu.edu/patroninfo.html
- Used html to create a link back to the SSO login for staff:



- Note: the ptype will not force users from this page to use SSO. Anyone can still use the name and barcode to access My Library Account via Courtesy Card User screen so it is not secure for library patron account information.

Innovative LSAP was nicer



- Note: the ptype would force campus community members to use LDAP credentials. Only community member ptype's could access My Library Account via Courtesy Card User prompt!

Innovative Pro Tip

- Pverify_web.html

- Access code via:
- http://sierra-app.bgsu.edu/screens/pverify_web.html

- Also you can see other's webpac config files with syntax:
- http://sierra-app.bgsu.edu/screens/wwwoptions

Innovative Single Sign On

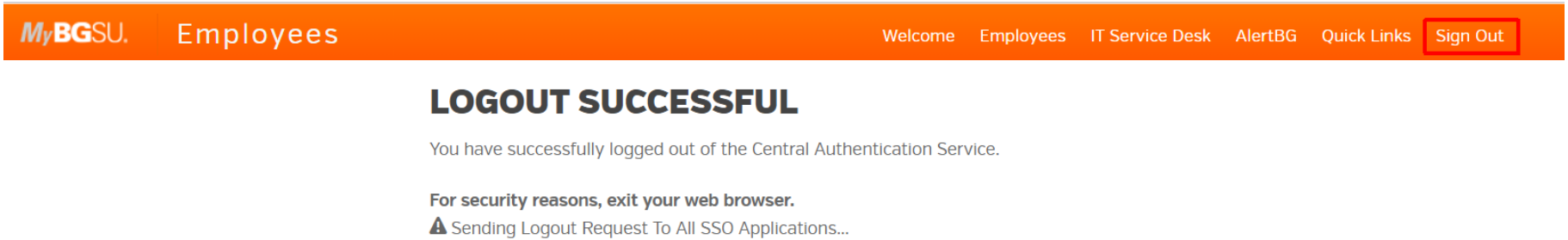
This SSO and https issue is still active

Sierra 4.3 Release Notes:
Libraries with SSO will not have HTTPS redirection. Compatibility between HTTPS redirection and SSO will be added in a future release.

https://iii.rightanswers.com/portal/app/portlets/results/viewsolution.jsp?solutionid=190122121139406&page=1&position=3

Innovative Single Sign On / Sign Off

My Central IT also desires that all single sign on software allow for a single sign off button (with closes all services signed it with single sign on)



Innovative Single Sign off has no way to accommodate this.
Set the SSO for the Innovative Apache credential to expire every 120 seconds or so. This does not effect users, but each 120 seconds in the background the Innovative SSO server will ping the campus SSO controller to issue new credentials.

Innovative Single Sign On

Questions?

Implementation: III Scheduler Product

- III scheduler product does not support public key authentication
- Scheduler requires username and password by typed in and saved

- BGSU ITS wrote to implementation staff when asked: “Public key authentication is a standard part of SFTP and is supported by nearly every SFTP client available as a more secure means for authenticating. Username/password authentication alone has been identified by most security experts as insufficient in adequately protecting the source of a connection request. BGSU is making a push to eliminate username/password authentication alone, specifically on interfaces handling user information or other automated transfers of data.”

Implementation / MyBGSU Portlet

Library Account At A Glance

Name: Strang, Mark J
Expiration Date: 5/27/2019
# of Items Currently Checked Out: 5
# of Items Currently Requested: 1

- To renew, cancel holds, or other actions, click here to go to your library account
- Questions about your account? Email circdesk@bgsu.edu or call 419-372-2051

Checked Out Items | Requested Items

Title	Due Date	Barcode	Call Number
Deliberate optimism	4/2/2019	A11359441018	LB2840
The confident teache	4/2/2019	A11360228172	LB2840
White fragility : wh	5/14/2019	3506500445581	HT 1521
Fame.	5/27/2019	A11352993825	M1508.M
Outrage in Ohio : a	5/27/2019	A11361174789	HV6533.

Showing 1 to 5 of 5 entries Previous 1 Next

My Library Account –My Millennium Web service protocols for campus portal view
https://techdocs.iii.com/mymillapi_patroninfo_object.php
https://csdirect.iii.com/sierrahelp/Content/sril/sril_patronapi.html

Implementation/Go Live

- Communication Plan
  - All Campus email
  - Social media
  - Library Home Page

  - What will be unavailable during conversion:
    Library Catalog Use OhioLINK catalog to find/view resources
    Patron Service: Renew books online/View My Library Account
    Library Service: OhioLINK book requesting
    Library Patron Service: Renew books
    Library Staff: check out books – paper circ
    Library Staff unable to work in Sierra
    Day of surprise issue announcements

Go Live

Initial Go Live: January 3, 2018

Actual Go Live: January 18, 2018

** Warning it can take some time for your DNS entries to propagate out to the broader internet. Off-campus users can be blocked for a few hours. Central IT says that is the nature of world wide web dns name managers. **

BGSU ITS erase, and dispose of old turnkey servers

Inn Reach SSO was not scheduled to happen on our implementation day even though we notified them we were an Inn-Reach partner

Go Live

Actual Go Live: January 18, 2018

AWS Firewall issues:

FTP service to campus Peoplesoft FTP server to use scheduler for automated Library Patron Load took a couple of days to get AWS ip's configured

PG Admin for MySQL wasn't opened through AWS firewall

On Positive side we choose to allow Sierra Web to only work for campus IP range so we wouldn't have students causing mischief from off campus

Staff need to use MYVPN to get to Sierra from off-campus

Post Go Live

- Uptime 13 months
- Maybe 6 brief outages, pretty awesome

- At least twice when an outage is longer than ten minutes I've called the help desk only to have it come back up while on the phone.
- Once the help desk knew about issue when I got through on the phone.

- Maybe 2 times its lasted 2-3 hours before coming back on line

- Launching sierra client can be slow after 12:00 est. –Normal network overload once west coast online and students activily at work

Questions?

Inn Reach SSO

- Differing user experience when requesting Inn Reach materials depending on where users start!

- Inn Reach Central Catalog/OhioLINK experience non-SSO
- http://olc1.ohiolink.edu

- Local catalog – SSO experience
- http://maurice.bgsu.edu

- Local Catalog experience non-SSO
- http://sierra-app.bgsu.edu

Inn Reach SSO

- Start at SSO server http://maurice.bgsu.edu if you pass along your local request from the central server you will be automatically get the SSO log in and get your campus SSO screen to authorize to fulfill your request. None SSO users need not apply
- wwwoption Inn Reach remote or Partner need to be setup for this

Inn Reach: Start request at central catalog

http://olc1.ohiolink.edu:80/record=b16334423~S0

(Search History) ▾ KEYWORD ▾ dancing till dawn: a century of ex Search

Record: Next ▸ *2 results found. sorted by date .*

Author	Malnig, Julie
Title	**Dancing till dawn : a century of exhibition ballroom dance / Julie Malnig**
Publish Info	New York : New York University Press, [1995], c1992

Bookmark this record as <http://olc1.ohiolink.edu:80/record=b16334423~S0>

Google Preview Limited Preview at Google Books

Library Holdings [Hide]

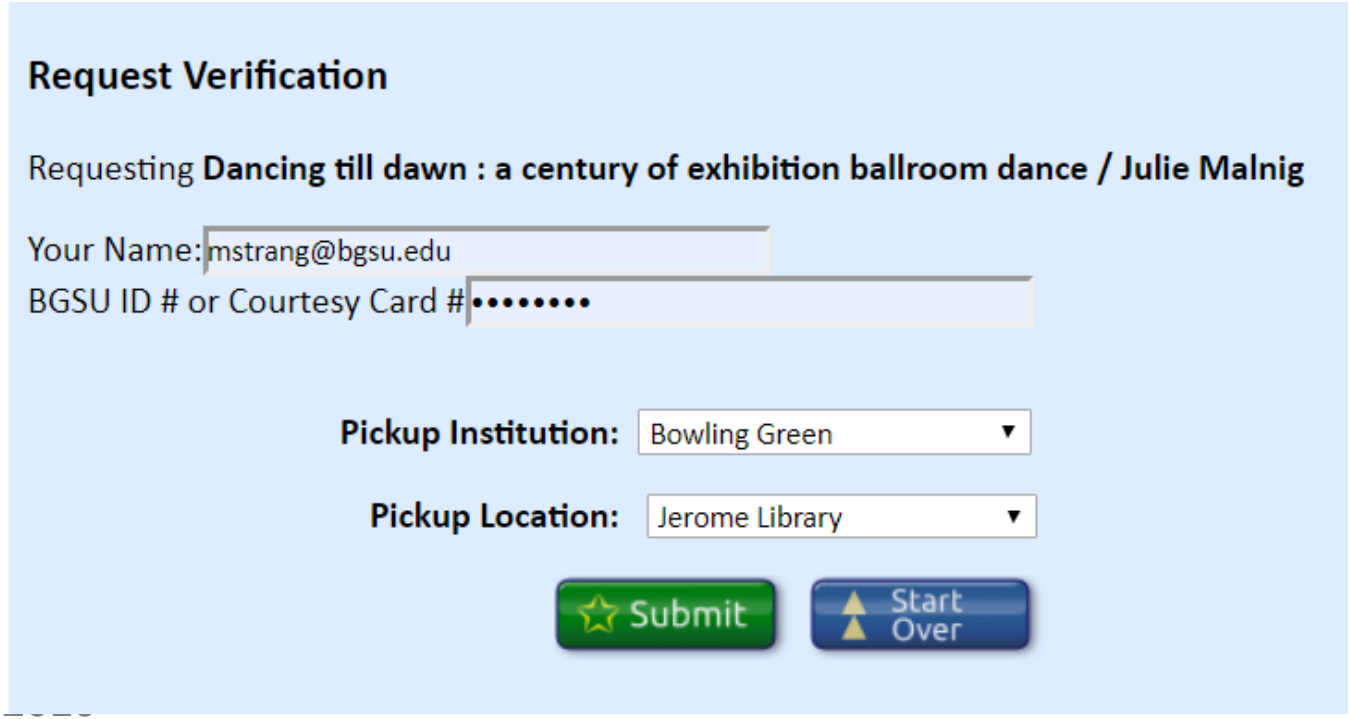
Request

Library	Location	Online Version	Call Number/Serial Holdings	Status
Denison University	DEN Main		GV1746 .M28 1995	AVAILABLE

[Go to top]

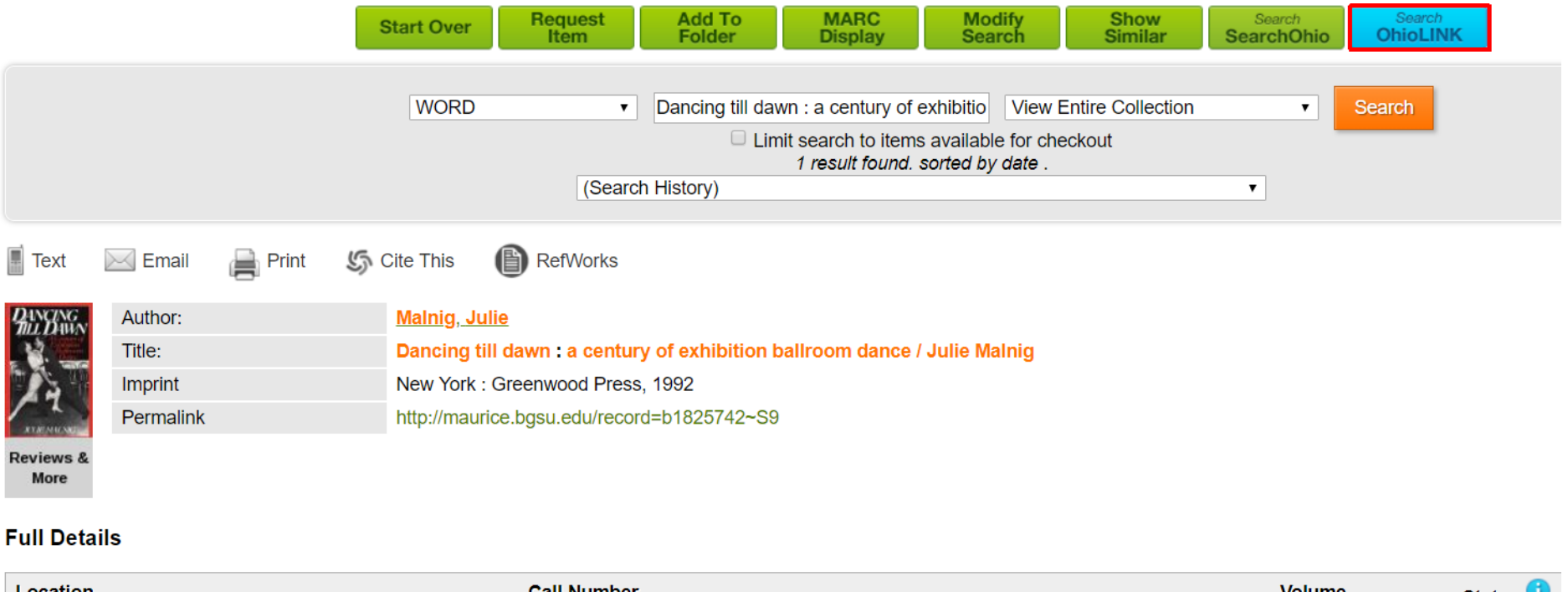
Inn Reach: Start request at central catalog

Request screen if start at OhioLINK url: https://olc1.ohiolink.edu



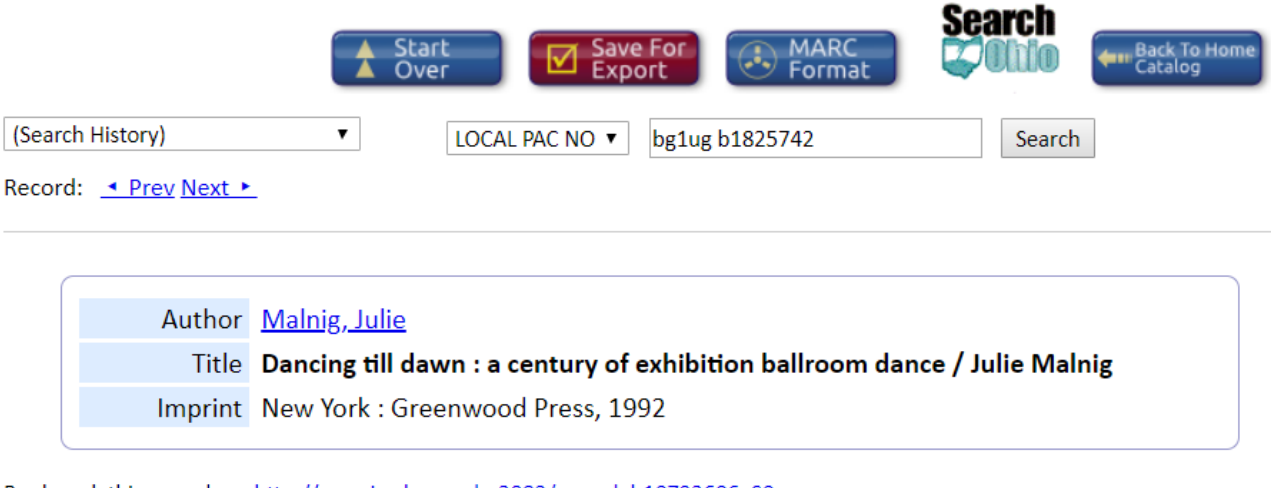
Inn Reach: Start request from local catalog

SSO Request screen if transfer from BGSU catalog to OhioLINK url:
http://maurice.bgsu.edu/record=b1825742~S9



Inn Reach: central url or courtesy card login screen

SSO Request screen if transfer from BGSU catalog to OhioLINK url:
http://maurice.bgsu.edu:2083/record=b10793606~S0

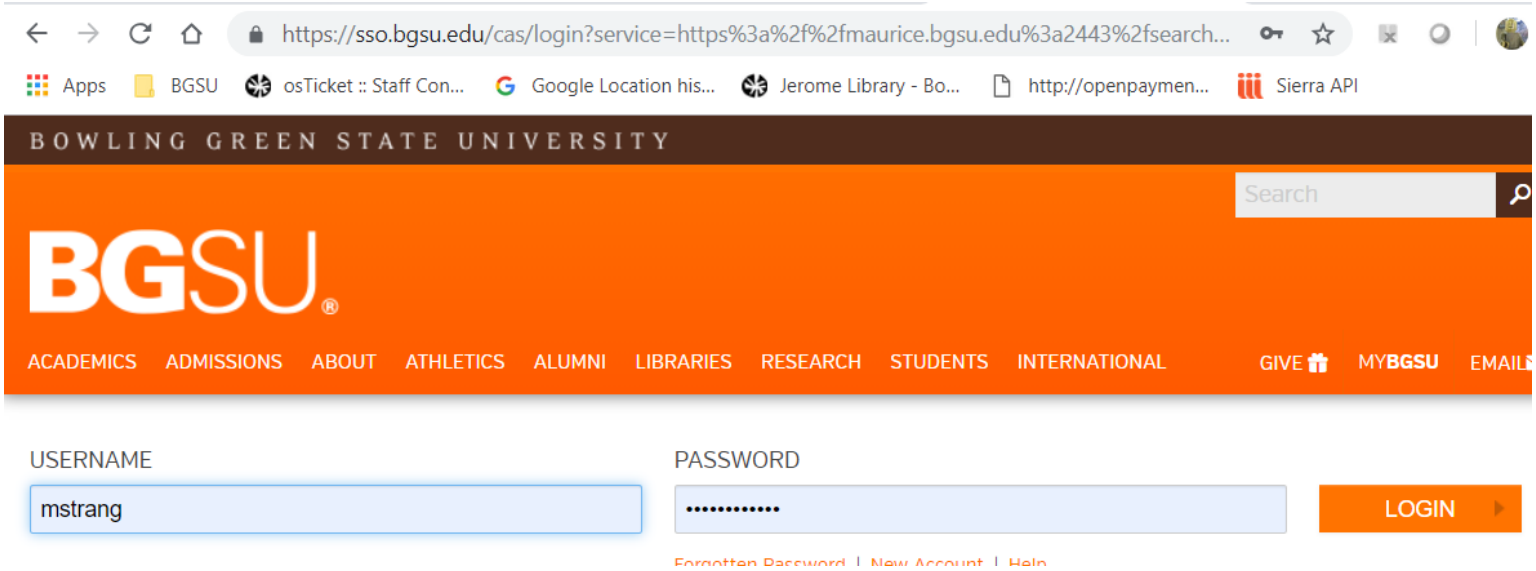


#IL

,AZ

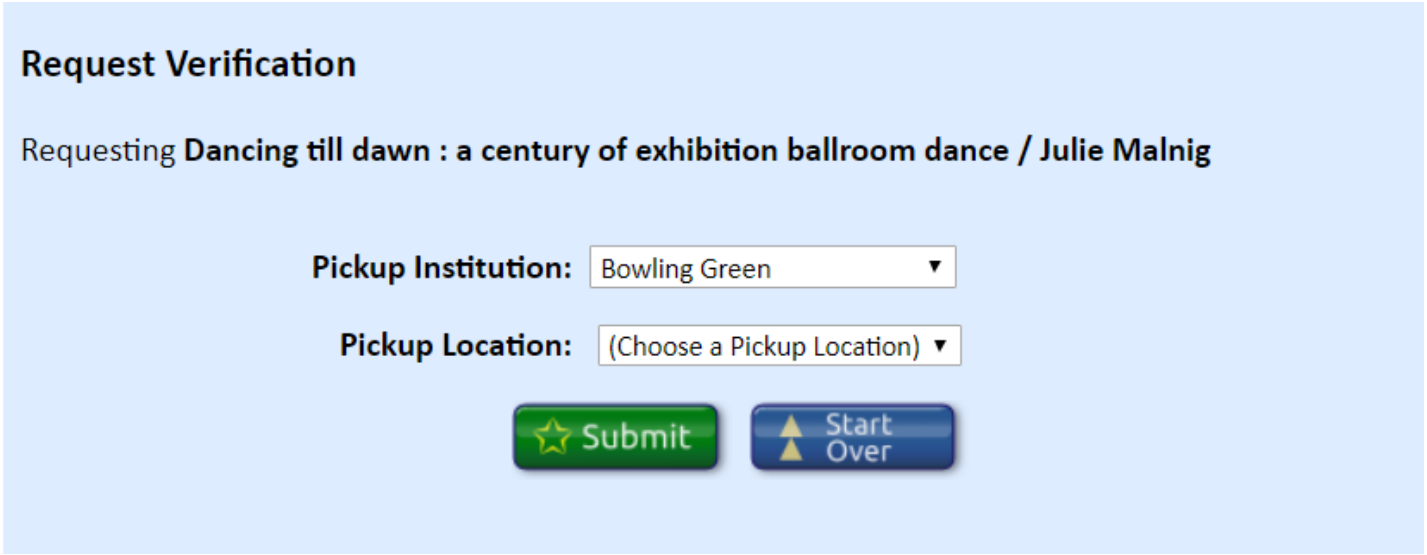
Inn Reach: central url or courtesy card login screen

SSO Request screen if transfer from BGSU catalog to OhioLINK url:
http://maurice.bgsu.edu:2083/record=b10793606~S0



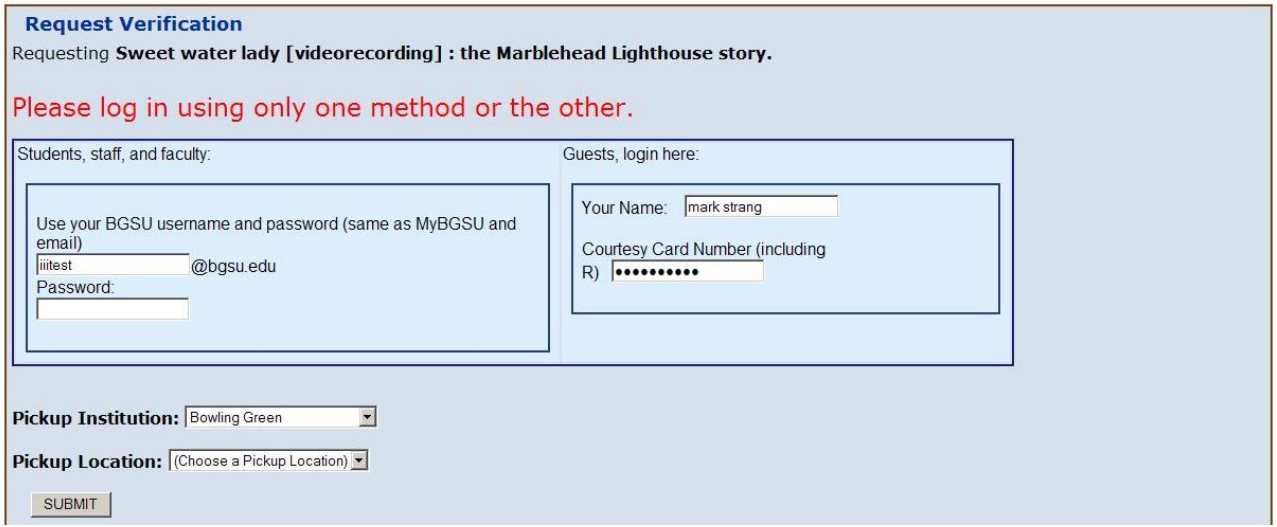
Inn Reach: central url or courtesy card login screen

SSO Request screen if transfer from BGSU catalog to OhioLINK url:
http://maurice.bgsu.edu:2083/record=b10793606~S0



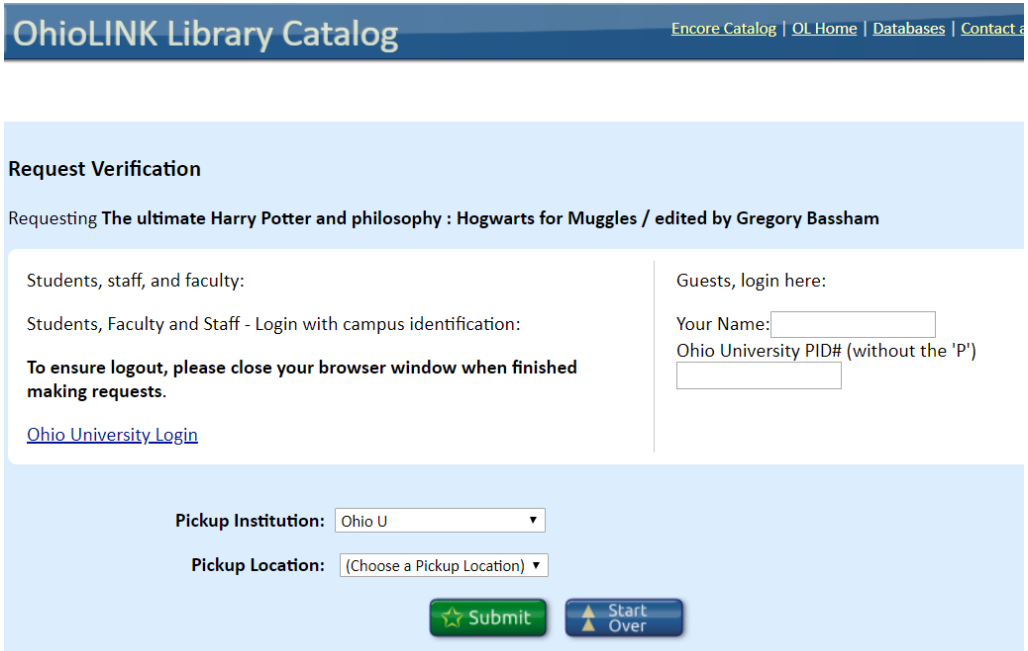
LDAP vs Inn Reach SSO

LDAP users at our central catalog get a split screen allowing them to login using either campus credentials or their name and university barcode:



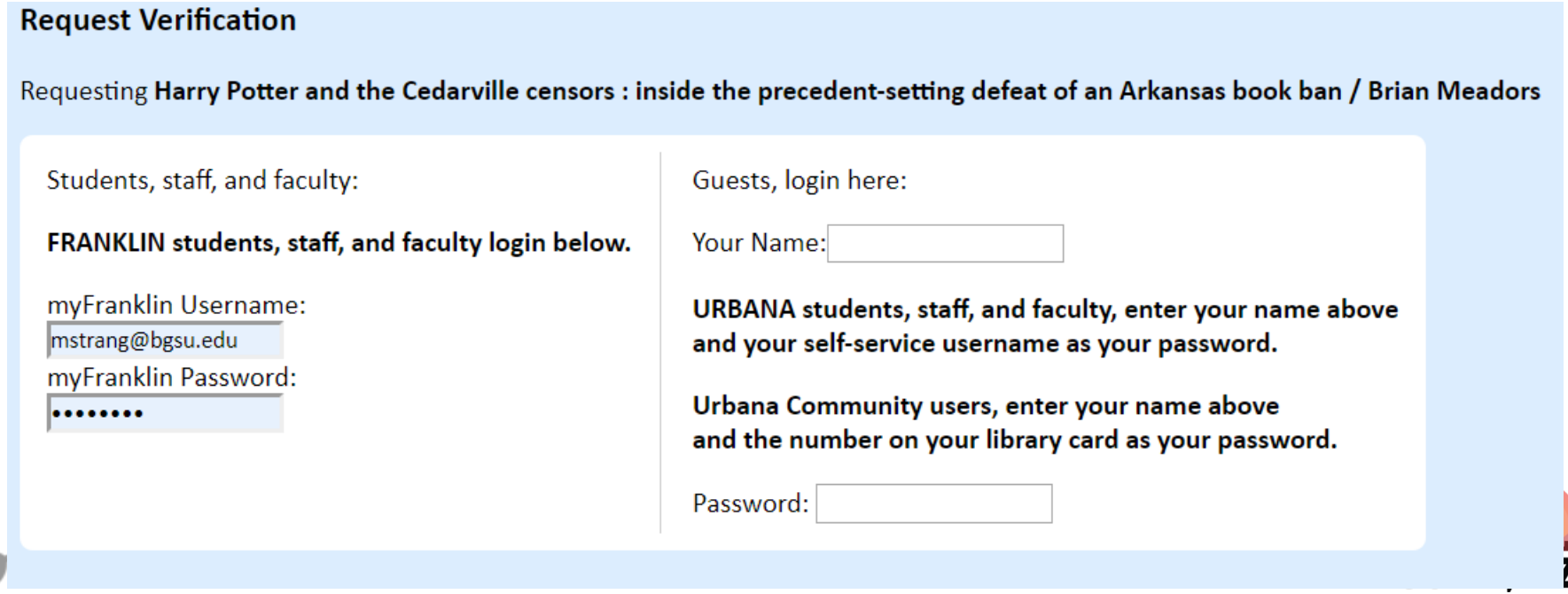
Inn Reach SSO

- Ohio University has gotten around the SSO limitation by using the LDAP split screen and javascript to pass search to SSO.
- I opened a ticket I've been told we can't duplicate this code



Inn Reach SSO / split screen

In preparing I talked with OhioLINK system admin and discovered a non ldap split screen that I hope is promising to improve.



Inn Reach SSO

Questions?

AWS Backup

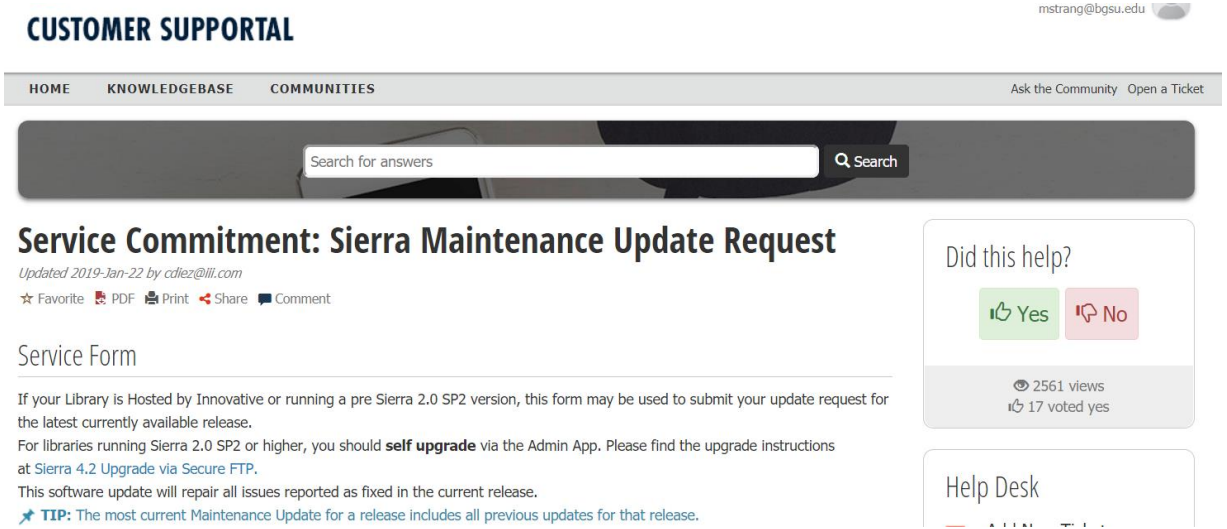
- With Innovative Cloud backup data is via SSL encrypted channel to encrypted storage at our US-based, SAS 70/SSAE-16 certified, cloud storage partner. Obviously the off-site data transfer is implicit in any cloud backup solution.
- Innovative will maintain and perform restores according as per our disaster recovery policy as part of support see: http://csdirect.iii.com/support/support_matrix.shtml
- Partial restores not covered in the disaster recovery can be performed but might be billable.
- Backups are performed 365 days a year at the agreed time.
- Backup times can be changed by contacting Support.
- There is a requirement for network bandwidth which can be defined and the throttled as not to affect the performance of the network
- Backup uses the Enterprise Backup API software. Notification via email are available after each backup if requested.

  - Innovative Cloud Backup FAQ
    https://iii.rightanswers.com/portal/app/portlets/results/viewsolution.jsp?solutionid=151129063722404&page=1&position=3

Sierra update

- Service Commitment: Sierra Maintenance Update Request
  - https://iii.rightanswers.com/portal/app/portlets/results/viewsolution.jsp?solutionid=160125103715462&page=1&position=1

No self updating your software to next release



AWS Firewall

- Service Commitment: Update SSH IP Address (III Hosted Systems)
  - Need to identify specific IP address for SQL access through iii
    We limited Sierra Desktop Client to the BGSU domain 129.1.*.* so no off-campus access unless staff use campus VPN

Sierra SAML future

- Sierra will have SAML Identity Provider (IDP)
  - Acts as master so other software can authenticate against Sierra
  - Initial testing underway

- Sierra will not have SAML Service Provider (SP)
  - Acts as servant so your software can authenticate against campus single sign-on without additional server
  - Innovative is aware of the need to do this development, however it is not a road map at this time
  - This is what we want so additional SSO server is not necessary

Advice if just starting

- Information to get from your Partners:

- Central IT
  - Do you allow LDAP to be used by third party hosted vendors?
  - Do you allow only one login screen for all SSO requests?
    - » How many sso implementations has local current expert done?

- InnReach
  - Do you allow custom InnReach requesting screen's for local sites
  - Inn Reach admin may not be aware that Innovative added some flexibility in recent years

Advice if just starting

- Identify the comfort level of Central IT for having a Virtual Machine with root, iiiroot, and outside vendor 24/7 access
- Budget in plenty of time to get your new Master License Agreement worked out between your legal office and Innovative
- Identify in advance if your Central IT will let you use LDAP on hosted servers.
  (Much better user experience for Inn Reach central catalog, and cheaper since no SSO server!)
- If go SSO, perhaps put SSO software onto a newly named server and then develop a split screen from application server for patrons who login
  - Will have dual url bookmarks for catalog
  - The method we used gives faculty a simple way to copy SSO url's into Learning Management System Courses (Canvas)
- Encourage Innovative to completely integrate new products with Inn Reach from the beginning

Thankyou!

Questions?

Mark Strang
mstrang@bgsu.edu