UH Applications Developers Meeting

04/04/2014

Michael Hodges, ITS, TI-IAM

Jodi Ito, ITS, Info Sec

Gwen Jacobs, ITS, CI

Sid Savara, ITS, MIS

Agenda

- Security Update: Overview of University of the Maryland Breach – a highly targeted attack
- Presentation: Utilizing a wiki space for organizing technical documentation
- Presentation: ITS Cyberinfrastructure: supporting the IT needs of the UH research community
- Presentation: UH Groupings, a versatile tool for authorizations management and much more
- Quick Tips
- End of Service Life Reminders
- Snacks: And an opportunity to meet your colleagues

Overview of the University of Maryland Breach – a highly targeted attack

Jodi Ito

Information Technology Security Officer

U-Md. computer security attack exposes 300,000 records

By Patrick Svitek and Nick Anderson, Published: February 19

More than 300,000 personal records for faculty, staff and students who have received identification cards at the University of Maryland were compromised in a computer security breach this week, school officials said.

The breach occurred about 4 a.m. Tuesday, when an outside source gained access to a secure records database that holds information dating to 1998.

Brian Voss, vice president and chief information officer at U-Md., said officials think that whoever got into the database duplicated the information, which includes names, Social Security numbers, dates of birth and university identification numbers for 309,079 people affiliated with the school on its College Park and Shady Grove campuses.

http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/19/ce438108-99bd-11e3-80ac-63a8ba7f7942_story.html

Highly Sophisticated, Highly Targeted Attack

The hackers did not change anything within the university's computer system, but Voss said the attackers essentially "made a Xerox of it and took off."

Voss said that what most concerns him is the sophistication of the attack: The hacker or hackers must have had a "very significant understanding" of how the school's data are designed and protected. Voss said the security breach appears to be in contrast with typical attacks, in which "someone left the door open," creating an easy opportunity for any hacker.

"That's not what happened here," Voss said. "There's no open door. These people picked through several locks to get to this data."

UNIVERSITY OF MARYLAND

OFFICE OF THE PRESIDENT

Main Administration Building
College Park, Maryland 20742
301.405.5803 TEL 301.314.9560 FAX

SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION
Testimony of Dr. Wallace D. Loh
President, University of Maryland
March 26, 2014

My name is Wallace Loh and I am the President of the University of Maryland. From its beginnings as a small, land-grant institution to its current status as a major presence in higher education, the University of Maryland has a long and distinguished history of excellence and innovation, evidenced by being #38 in the 2013 Academic Ranking of World Universities.

I am grateful for this opportunity to discuss an issue that is not only important to the higher education community but to all of us who participate in online activities on a daily basis. As the state's flagship institution, the University of Maryland has 37,000 students, 12 colleges and schools, 9000 faculty and staff, and an annual $1.7 billion operation budget. To safeguard such a large and complex operation, we recently doubled the number of our IT security engineers and analysts as well as our investment in top-end security tools. However, as our recent data breach reveals, more remains to be done.

On February 18, 2014, the University of Maryland was the victim of a sophisticated computer security attack that exposed records containing personal information of faculty, staff, students and affiliated personnel from the College Park and Shady Grove campuses. Fortunately, no financial, academic, health or contact (phone and address) information was compromised, but we are not taking any chances. I have ordered five years of credit protection services at no cost to every person affected by this breach. This is above and beyond the protection measures taken by other organizations and institutions, and so far nearly 30,000 persons affected by the breach have registered, which is also well ahead of projections. In addition, all sensitive records in the breached database that are no longer required have been removed.

http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=b92bba0e-787f-426d-b1ce-14f2c73f9f13

Congressional Hearing Webcast

"Protecting Personal Consumer Information from Cyber Attacks and Data Breaches"

President Loh's testimony about 45 minutes into the webcast:

http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=082407f8-9740-4e43-b2d2-1520c5495014&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a

March 27, 2014

Univ. of Maryland hackers used trojan to steal IT credentials, access database

Share this article:

University of Maryland President Wallace Loh appeared before Senate members to testify on the occurrences leading up to a far-reaching breach.

According to Loh, who spoke Wednesday, hackers masking their identity and whereabouts with the Tor network, infected a university website with a data stealing trojan.

After compromising the photo sharing site, saboteurs were then able to steal login credentials of IT managers at the university, and access a trove of information located in a database – the names, Social Security numbers and university identification numbers of 300,000 University of Maryland students, alumni and staff.

The university president told Senate members that the attackers cloaked their activity by using Tor.

http://www.scmagazine.com/univ-of-maryland-hackers-used-trojan-to-steal-it-credentials-access-database/article/340117/

Morning Security Brief: UMD Data Breach Update, GAO Report on Critical Infrastructure, and Job Sites Hacked

By Lilly Chapa

03/27/2014 - ► In the month since hackers stole personal data of 310,000 students, faculty, and staff involved with The University of Maryland, the school has moved most of its Web sites to the cloud, expunged 80 percent of its databases, and hired experts to improve its protections, UMD president Dr. Wallace Loh told Congress yesterday. However, since the attacker used the anonymous browser Tor, nobody may ever be caught for the data breach, according to WUSA. Loh told the Committee on Commerce, Science, and Transportation that the hacker uploaded a Trojan horse to a university Web site meant for uploading photos. The malware found the passwords for some IT managers, which gave the hacker full access to troves of personal information dating 20 years back. UMD has offered five years of free credit monitoring to victims, Loh said.

http://www.securitymanagement.com/news/morning-security-brief-umd-data-breach-update-gao-report-critical-infrastructure-and-job-sites-

Attack Methods

- Public website to upload photos was used to upload malicious software
- Hackers gained access to scripts used to change passwords on LDAP
- Hackers also identified who IT admins were and gained access to their accounts
- Eventually gained access to DBA account for ID card management database and exfiltrated data via TOR node
- Database contained accumulated information (old information was never purged)

UMD Lessons Learned

- Remove servers and services that are not needed
- Patch software in a timely manner
- Architect environment appropriately (separate web server from database server)
- Ensure that only necessary personnel have proper access (remove access and accounts when not needed)
- Investigate two factor authentication
- Check file permissions regularly
- Know what is in your databases and ONLY KEEP DATA THAT IS NEEDED
- Check firewall rules allowing only authorized individuals access and tighten rules as much as possible

Adam Greenberg, Reporter

Follow @writingadam

http://bit.ly/1neWJrm

February 28, 2014

Files containing 360 million credentials, 1.25 billion email addresses, located on Deep Web

The number of individuals impacted in data breaches is skyrocketing.

In the first three weeks of February, Hold Security – a company that aided in discovering a number of breaches, including Adobe – has located more than 20 data files on the Deep Web that together contain roughly 360 million email addresses with passwords, and about 1.25 billion email addresses alone.

“In sheer numbers, this is a major change in what we've seen being reported,” Alex Holden, CISO at Hold Security, told SCMagazine.com on Friday, explaining it may stem from a significant increase in the number of online accounts over time. “Even if you have a success rate that is a fraction of a percent, it's still a huge number,” he said.

The biggest file Hold Security unearthed on the Deep Web in February contained 105 million email addresses and passwords, Holden said, but added that, as with all 22 caches of credentials discovered by the company, the data in each file could be the product of multiple breaches.

Questions?

Jodi Ito

Information Technology Security Officer

Utilizing a wiki space for organizing technical documentation

Sid Savara
KFS Team Manager
and Software Developer

Summary

- KFS Uses Confluence/Wiki A Lot
- Filters, Gadgets, Macros Allow Us to Use **1 Screen** to Make Decisions
- (We use it for normal wiki stuff too)

Why Use Any Tool/Tech?

Solve One Or More Problems

So What Are We Solving?

NOT A Problem

Get This "Stuff" Organized

(This Isn't A Real Problem)

Why Are We Organizing?

Solve These Other Problems….

Problem Summary

1. Stand-In For Training
2. **Solutions Cheat Sheet**
3. **Serve As Proxy for OOO**
4. Shared Knowledge Base
5. Contracts

Why Confluence (vs. Gdoc, Word)

1. Gadgets / Summarizing/Scripts
2. Filters to Pull In via JIRA
3. Formatting *(debatable)*
4. Templates *(not demoed today)*
5. Online Availability
6. Easy Linking Between Pages
7. Versioning

Examples of Basic Use (Quick)

1. Developer Set Up Guide
2. Tutorials/Cheat Sheets
3. OOO/Standard Procs
4. Knowledgebase/Reference/ Contract

Ex: Training - iReport

Creating Your First iReport

Created and last modified by Norman Y Saruwatari on Mar 24, 2014

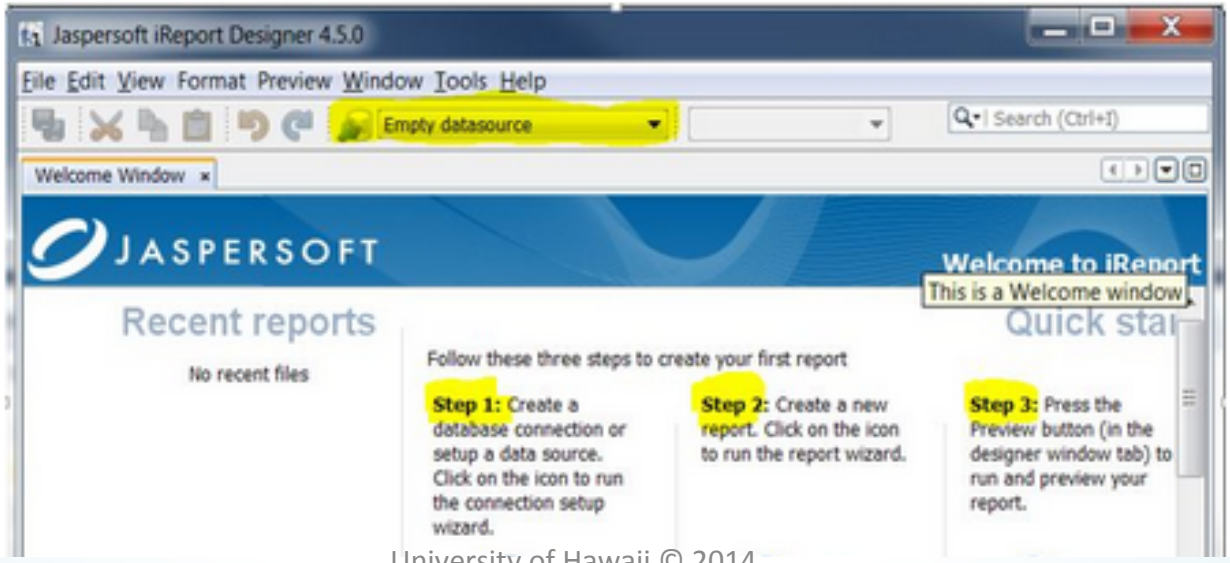
- Introduction (*** Page Under Contruction ***)
- Step 1: Create a Connection/Data Source

Introduction (*** Page Under Contruction ***)

To create

Step 1: Create a Connection/Data Source

1. Start iReport.



Ex: Solutions Cheat Sheet #1

- MIS Developer Notes
  - Adding a Lookup to a Text Control
  - Adding an Extended Attribute - A Case Study (Part 1)
  - Adding an Extended Attribute - A Case Study (Part 2)
  - Adding an Extended Attribute - Additional Stuff
  - Advanced Confluence Tricks
  - CAS Integration (Prod CAS)
  - CAS Integration (Test CAS)
  - Creating CSVs in KFS Open CSV

Ex. : Dev OOO

How To Promote SVN Revisions Between Branches

Created by Travis Schneeberger, last modified by Siddartha Savara on Aug 02, 2013

- Overview
- Subclipse SVN Merge
- SVN diff/patch
- Manual Compare
- Frequently Asked Questions (FAQs)
    - Reverting Conflicts
    - Resolving Conflicts
    - Why Update Trunk When Merging to Test?
    - SVN Status Codes
    - Reverting Conflicts

Ex: Shared KB – Env Status

Production

Environment	Website	App Server	Dat
Production	http://kfs.hawaii.edu/kfs-prd	kfs01.pvt.hawaii.edu kfs02.pvt.hawaii.edu kfs03.pvt.hawaii.edu; 16 GB, 2 vcpu	kfs

Load Testing

Environment	Website	App Server
LT	http://www.test.hawaii.edu/kfs-lt	kfs12.pvt.hawaii.edu kfs13.pvt.hawaii.edu;

Ex. : Contract

Kuali Financial System Technical / ... / Jasper Reports

Jasper Standard Report Format

Created by Tammy-lu Vandevender on Mar 24, 2014

The KFS Reporting Team has developed these guidelines in developing Jasper re

Format

Font name:	Courier New
Font size:	8
Cell(Line) height:	10
Page Orientation:	Horizontal
Scripting language:	Groovy
Margins:	20 pixels (Top, Bottom, Left, Right)

Demo: KFS Batch Jobs

1. Main Job Page
   - Dynamically Create Lists
2. Single Job Page
   - Contains Macros That Build It
3. Gadgets
   - Pull Solutions From JIRA

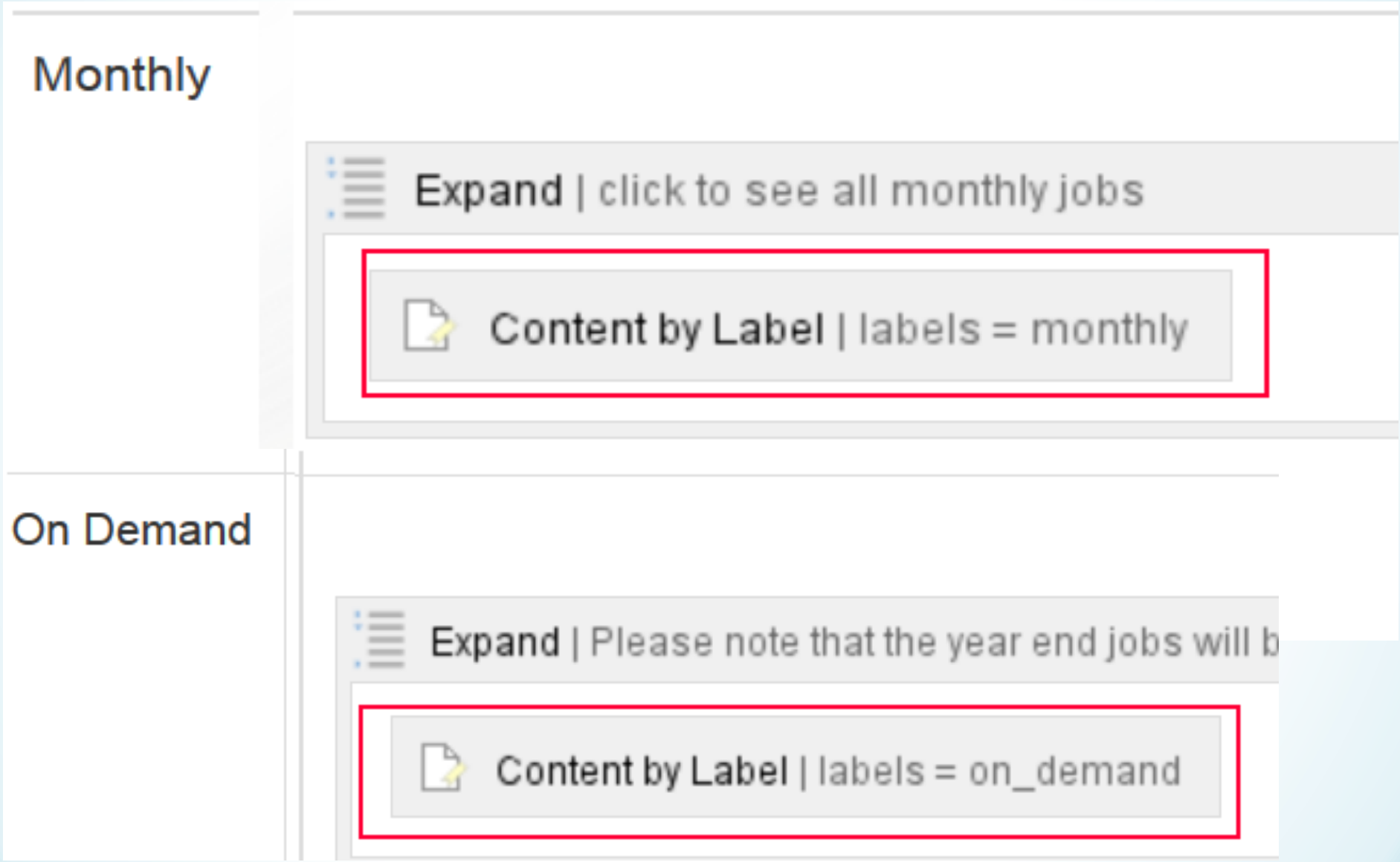
Ex: Organize By Labels (1 of 3)

Main Benefit

- Labeling Lets Us Group Things
- Avoid Duplication of Effort: Tag It, Automatically Listed

Ex: Organize By Labels (1 of 2)

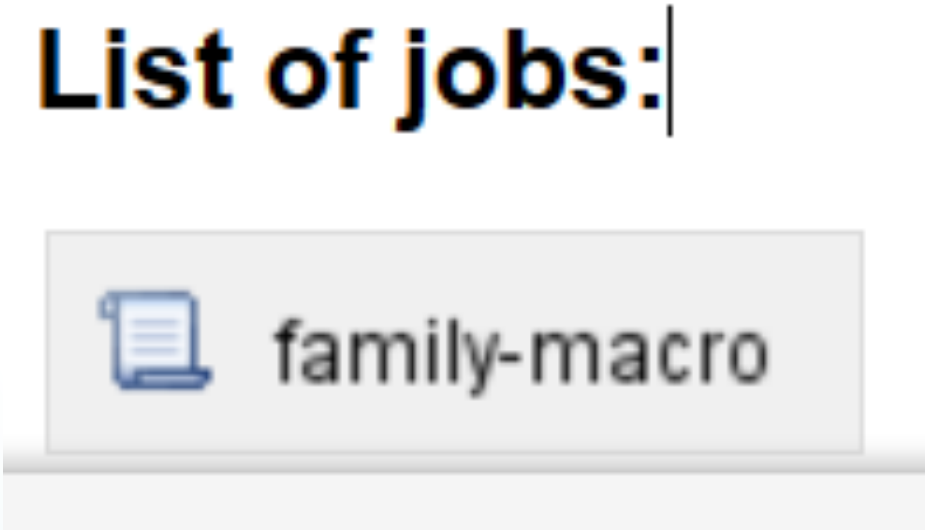
Ex: Organize By Labels (2 of 2)



Ex: Dynamic List By Macro

(Too Big To Demo)

Similar to Organize By Label

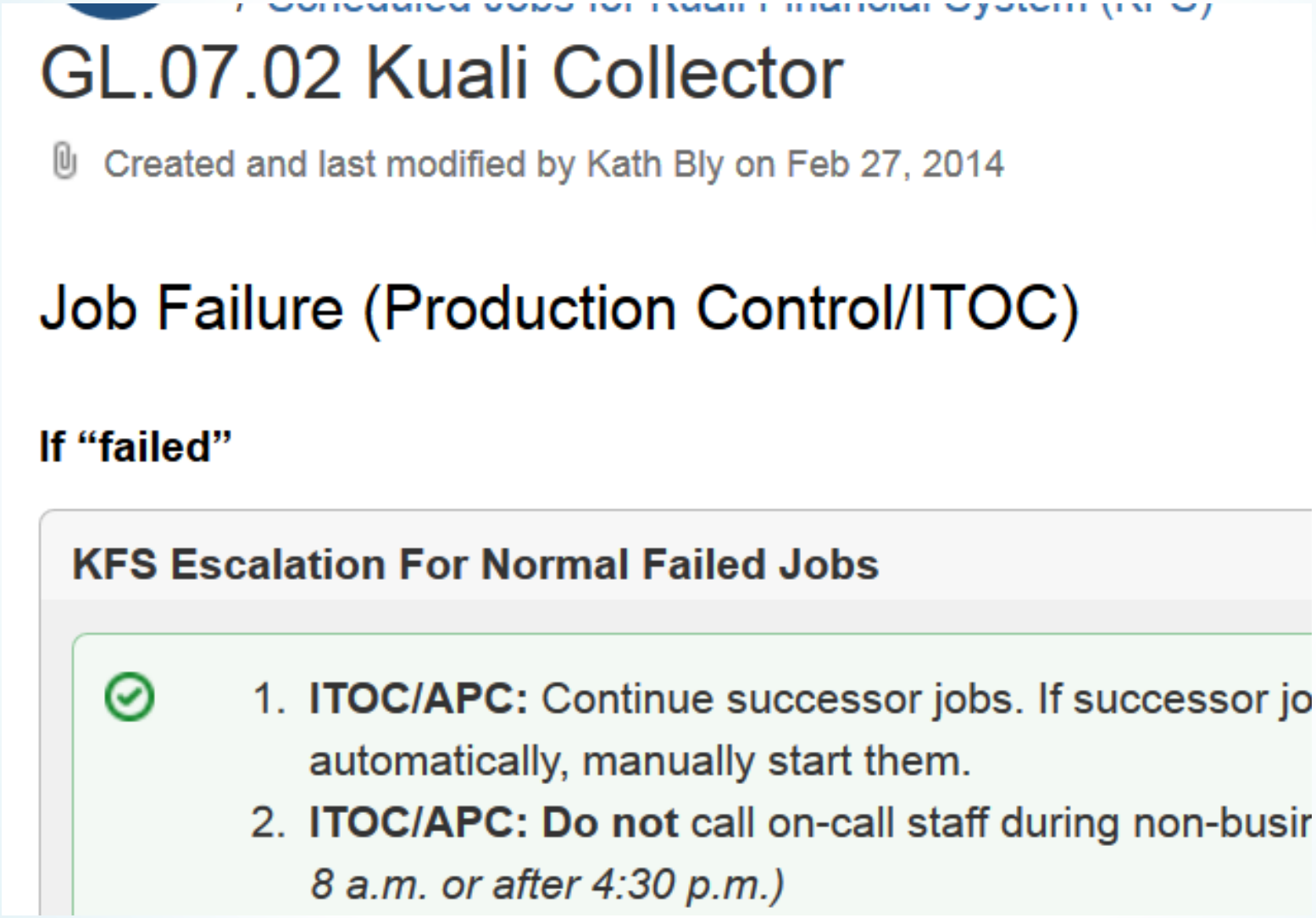


Ex: Include Excerpts (1 of 3)

Main Benefit

- Can Duplicate Content Across Many Pages
- Makes a Single Page Printable
- *(Alternative is Linking)*

Ex: Include Excerpts (2 of 3)



GL.07.02 Kuali Collector

Created and last modified by Kath Bly on Feb 27, 2014

Job Failure (Production Control/ITOC)

If "failed"

KFS Escalation For Normal Failed Jobs

1. **ITOC/APC:** Continue successor jobs. If successor jo
   automatically, manually start them.
2. **ITOC/APC: Do not** call on-call staff during non-busir
   8 a.m. or after 4:30 p.m.)

Ex: Include Excerpts (3 of 3)

Job Failure (Production Control/ITOC)

If "failed"

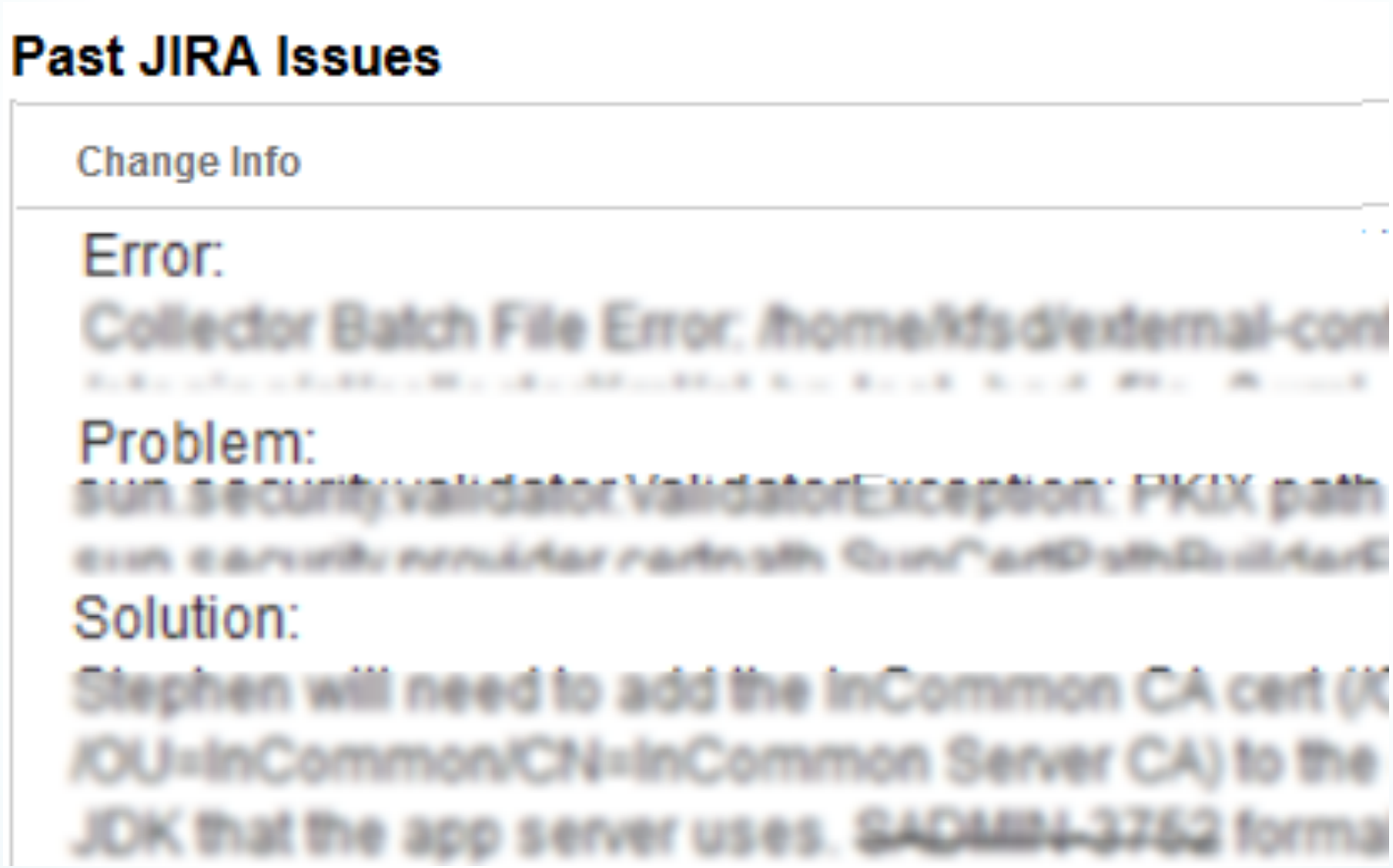
Excerpt Include | KFS Escalation For Normal F...

Ex: Filter Gadget (1 of 3)

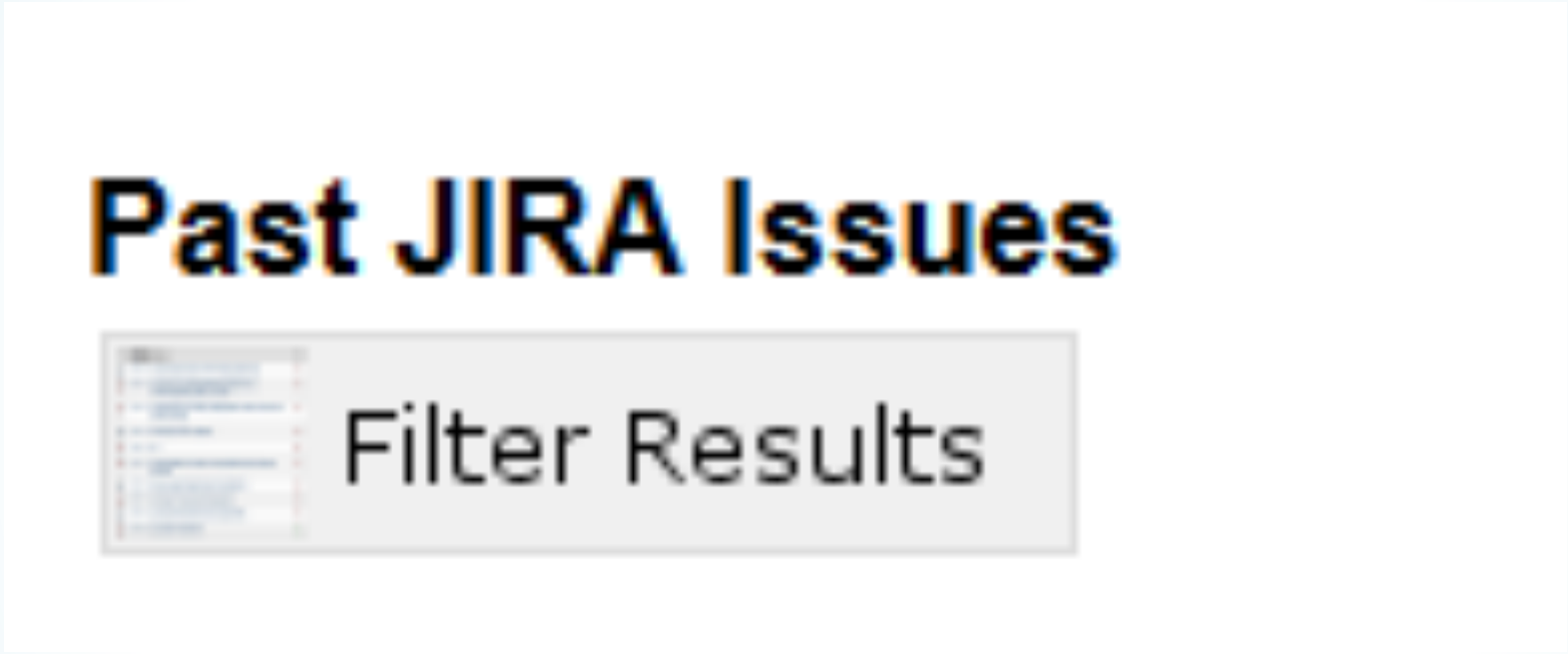
Main Benefit

- Pull Troubleshooting Info From JIRA (Bug/Issue Tracking)
- Single Page W/ Job Info

Ex: Filter Gadget (2 of 3)



Ex: Filter Gadget (3 of 3)



That's It

- Wiki Is Not Just Static Content
- Gadgets/Filters/Macros Make It Easy To Build Powerful Pages

Questions?

Sid Savara
KFS Team Manager
and Software Developer

ITS Cyberinfrastructure: supporting the IT needs of the UH research community

Gwen Jacobs

Director for Cyberinfrastructure

UH Cyberinfrastructure (CI) Goals

- Implement advanced CI Framework to support the research mission: HPC, software, data storage and analysis, visualization, professional staff scientists
- Recruit CI research scientists and establish support and training activities for faculty and students
- Partner with colleges, schools and research centers to support research activities – avoid duplication, aggregate and consolidate shared services, save energy
- Pursue collaborative funding opportunities and develop sustainable support mechanisms for research cores

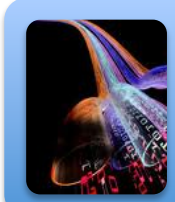
Cyberinfrastructure investments in progress

Dedication and blessing of the Information Technology Center
December 16, 2013

UH Information Technology Center

Data Center

- 8000 sq ft
- Virtual machines and colocation services
- HPC and large scale data storage

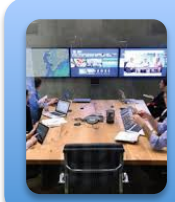


Networks

- 40G to National R&E Networks
- NSF CC-NIE Award: 10gig campus upgrade
- Connect research labs with UH Data Center

High Performance Computing

- $2M Compute Cluster Acquisition



Collaboration suites

- Emergency Situation Room
- Videoconferencing suites/ meeting rooms

CI Research Scientists

- NSF ACI-REF Program
- National Consortium best practices
- Clemson, Harvard, UH ,USC, UWisc, UUtah

UNIVERSITY of HAWAI'I SYSTEM

University of Hawaii © 2014

Partnerships supported by cyberinfrastructure

- Research Infrastructure Programs
  - INBRE, COBRE, RCMI, EPSCoR
- Colleges, Schools, Research Centers and Institutes
  - Shared core facilities
    - High Performance Computing
    - Large Scale Data Storage
    - Co-location and virtual machine services
    - Software, scientific workflows, visualization
    - Expertise: research scientists
- Current infrastructure grants: 2013 - 2016
  - NSF CCNIE: 10 gig Campus Network upgrades to support research
  - NSF FSML: End to end CI support at Hawai'i Institute of Marine Biology
  - NSF ACI: National Consortium: Advanced CI Education and Research Support
    - Institutions: Clemson, Harvard, UHawai'i, USC, UWisconsin-Madison, UUtah

Advanced CI Support for major funding initiatives

- Hawai‘i EPSCoR – Track 1
  - $20M; Five year award: Center of Excellence
  - Data Intensive Science and Engineering Theme
    - Hire faculty, postdocs, research scientists in data science methodologies
    - Support 3-5 research grand challenges
    - Training for faculty, students – workshops/summer school
    - Undergrad curriculum efforts
  - Research Cores
    - Informatics – Bioinformatics, Ecoinformatics
    - High Performance Computing
    - Big Data Analytics
    - Data Management
    - Visualization

Questions?

Gwen Jacobs

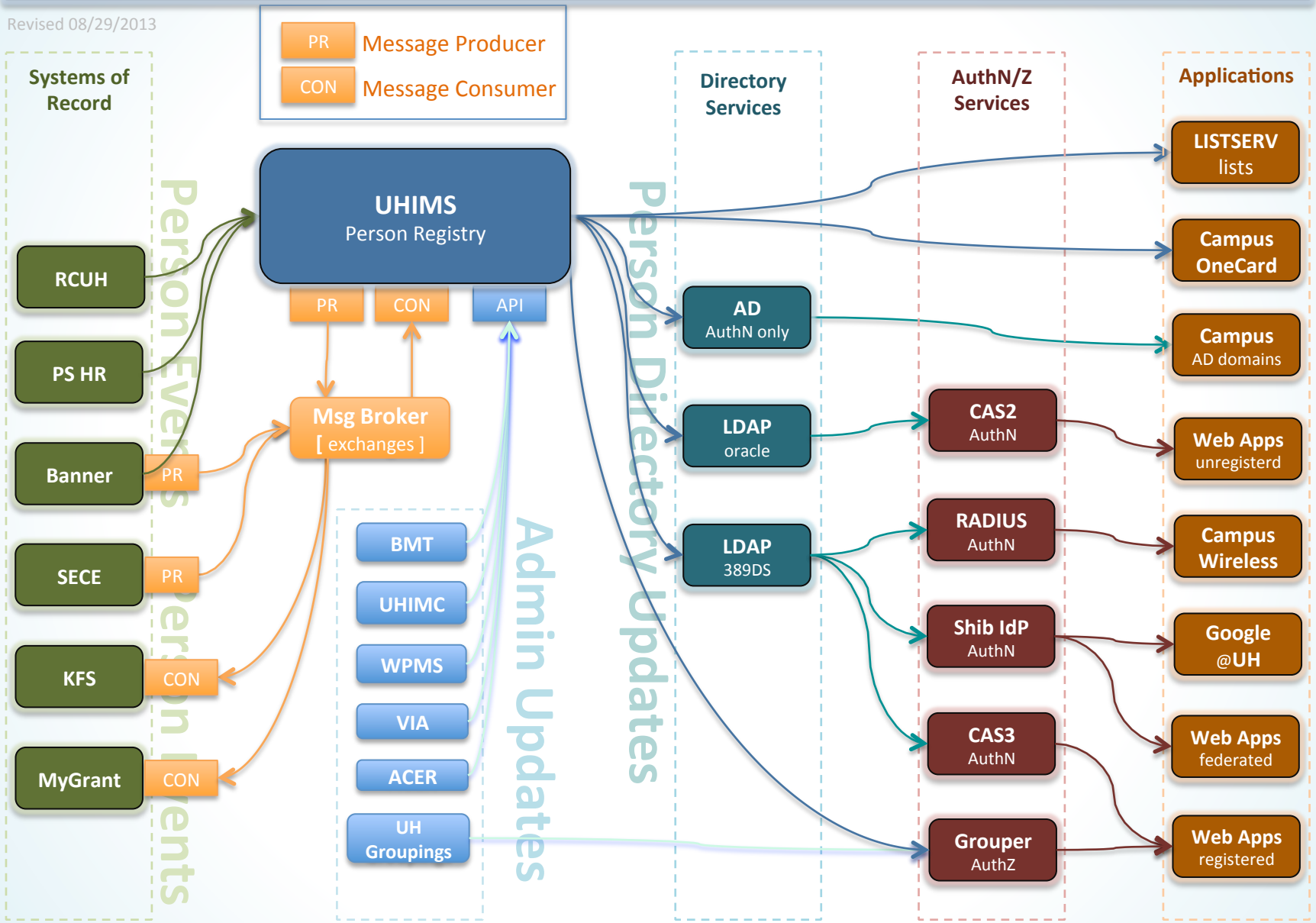
Director for Cyberinfrastructure

UH Groupings, a versatile tool for authorizations management and much more

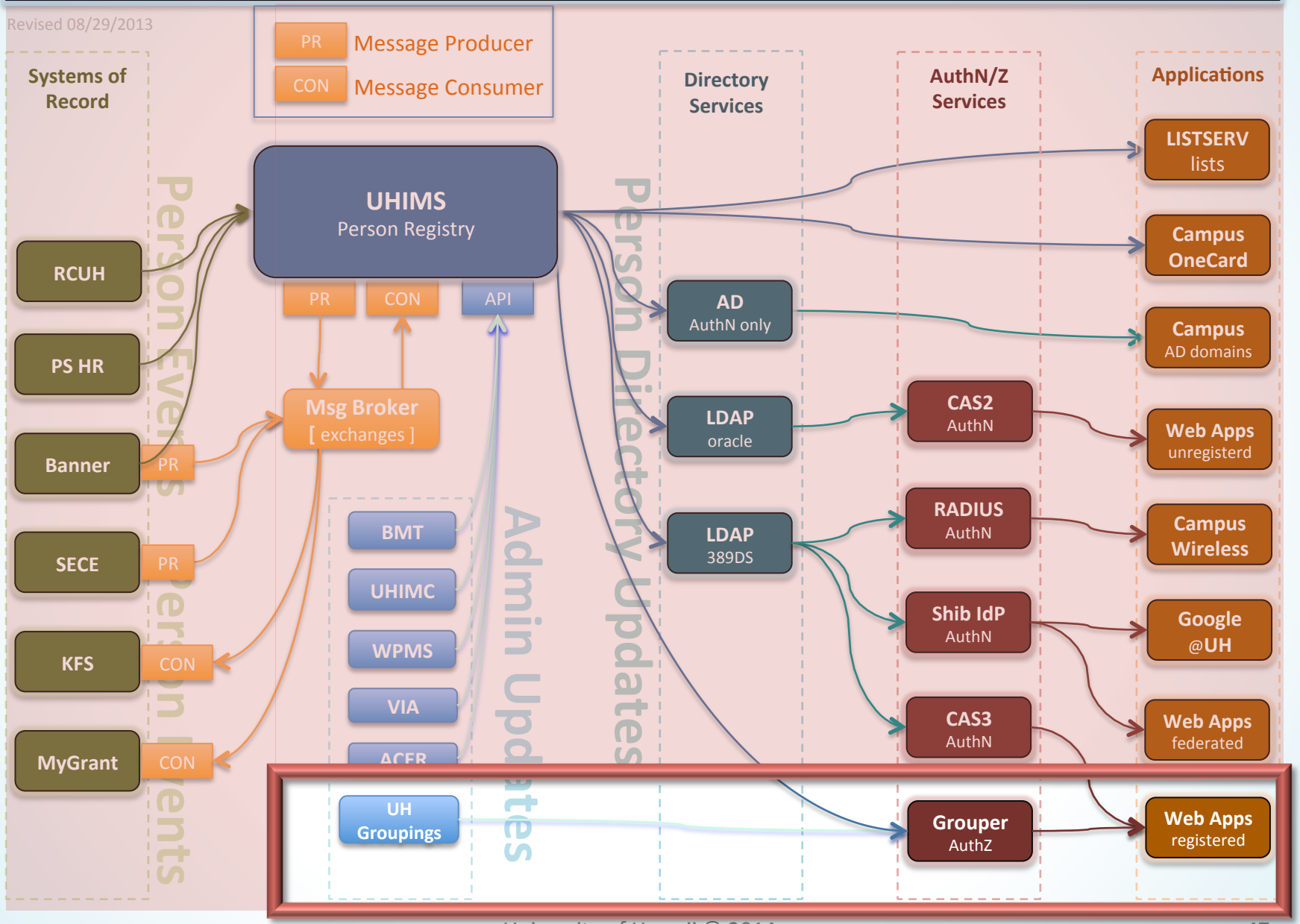
Michael Hodges

Identity and Access Management Team Manager

UHIMS Ecosystem (circa 2014)



UHIMS Ecosystem (circa 2014)



UH Groupings

- What are we grouping?
  - People, members of the UH community.
    (A UH Number is a prerequisite.)
- Why are we grouping?
  - Groupings imply roles, imply entitlements.
  - ***Automation is available.*** Business rules can be used to help create and manage Groupings.
- How are Groupings created?
  - Automatically by UHIMS.
    (Thanks to connections with Banner, PeopleSoft HR, RCUH, SECE, etc.)
  - Manually, some things require the human touch.

UH Groupings, Concepts

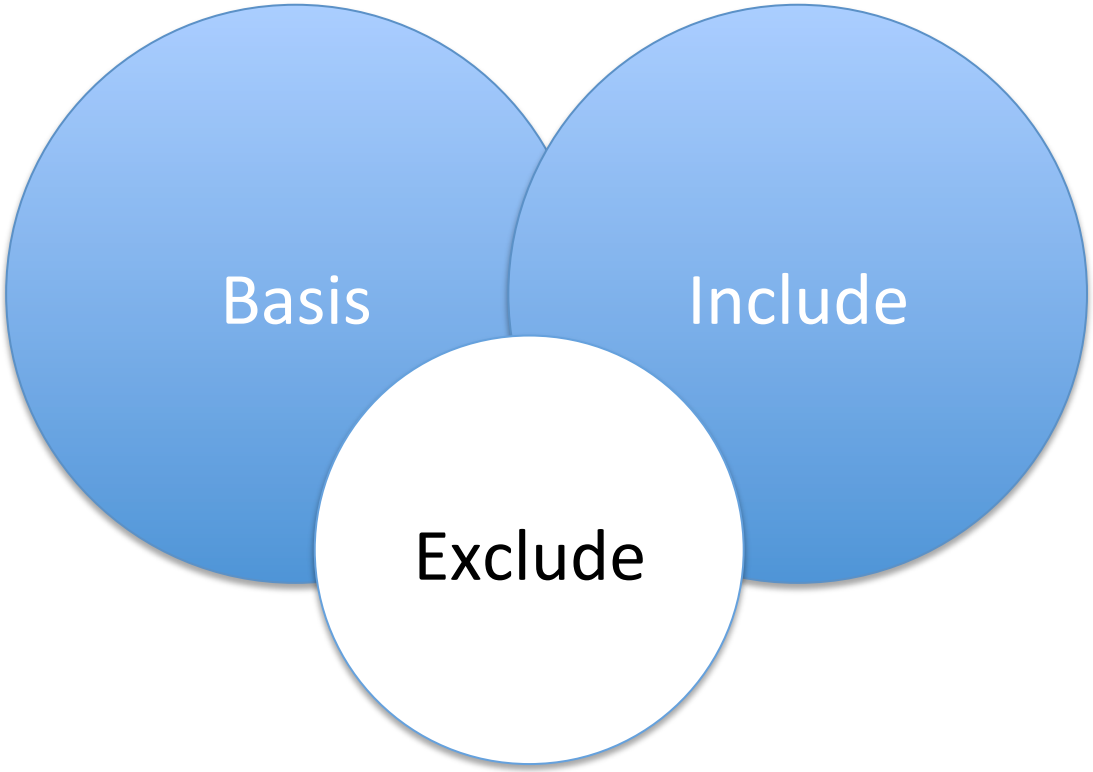
- A Grouping
  - Is a simple or complex expression of membership
  - Is composed of 3 groups, conceptually
    - Basis, Include, Exclude (more on this in a moment)
  - Has 1 or more Owners
  - Has properties that an Owner can configure
  - Is reusable, can serve multiple purposes
    - Application authorization (who can do what)
    - LISTSERV list publication (email notifications)

UH Groupings, Concepts

- A Grouping is composed of 3 groups, conceptually:
  - **Basis** group (e.g.: UHH Faculty) (may be empty)
    - Populated using automatically populated groups that reflect your core requirements.
  - **Include** group (may be empty)
    - Ensures member inclusion, regardless of the Basis.
    - Populated manually or via a campus application.
  - **Exclude** group (may be empty)
    - Ensures member exclusion, regardless of Basis/Include.
    - Populated manually or via a campus application.
  - In Set Theory: ((Basis U Include) \ Exclude)

UH Groupings, Concepts

(Basis U Include) \ Exclude

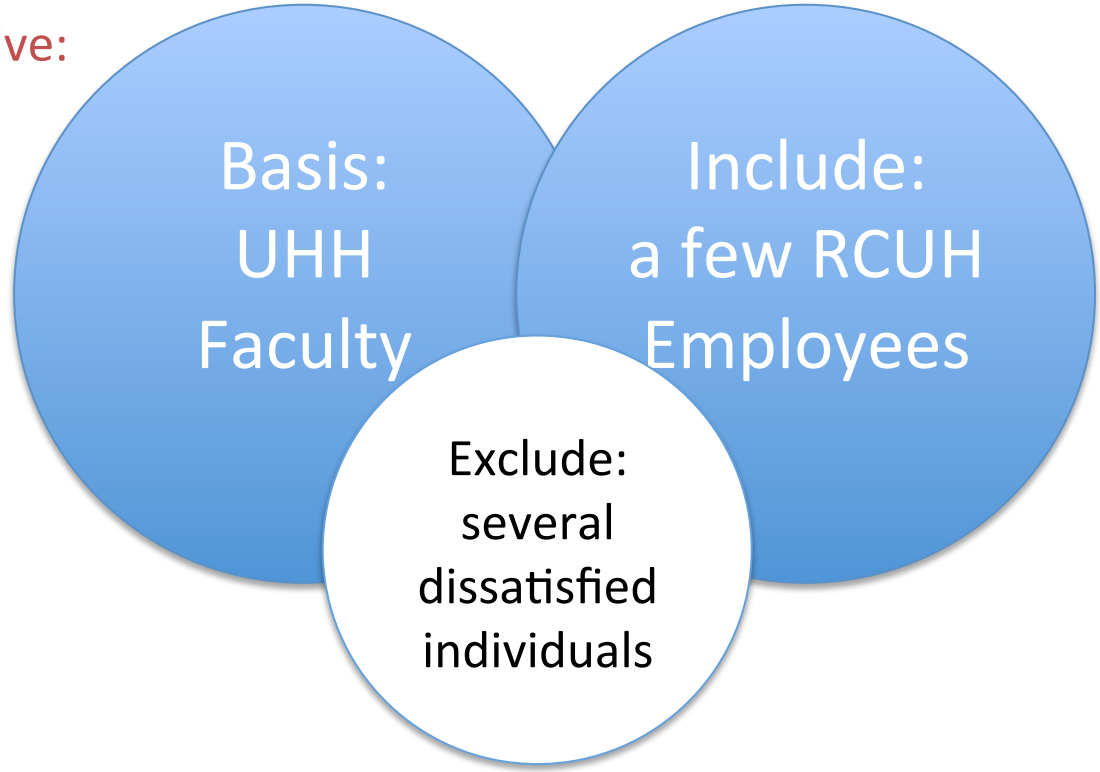


UH Groupings, Concepts

(Basis U Include) \ Exclude

Sample objective:

implement a campus mailing list



This design maximizes flexibility and facilitates the implementation of an easily understood user interface.

UH Groupings

- Simple Basis Group examples:
  - Maui CC students, faculty, lecturers, staff, retirees
  - RCUH staff
  - UHM faculty librarians
  - UH System civil service employees
  - KCC student employees, work study students
  - UHM grad students in the law school
  - LCC students enrolled in IS 100 CRN 54588, Fall 2014
  - Hilo students seeking a Nursing BS
  - UHM student seeking a JD

UH Groupings

- Compound Basis Group examples:
  - ITS civil service employees:

    Group: …hris.eac.2213460

    INTERSECT

    Group: …uhsystem::staff.civilService
  - ITS employees that are students (tuition waivers?):

    Group: …hris.eac.2213460

    INTERSECT

    Group: …sis.20143:enrolled

UH Groupings, Roles

- Owners
  - Successfully request a UH Grouping.
  - Manage the Grouping's list of owners.
  - Add/remove members from the Include group.
  - Add/remove members from the Exclude group.
  - Enable/disable members' Opt-In Self-Service option.
  - Enable/disable members' Opt-Out Self-Service option.
- Members
  - If allowed, may include/exclude themselves.
  - Receive email, if the Grouping is published to a LISTSERV list.

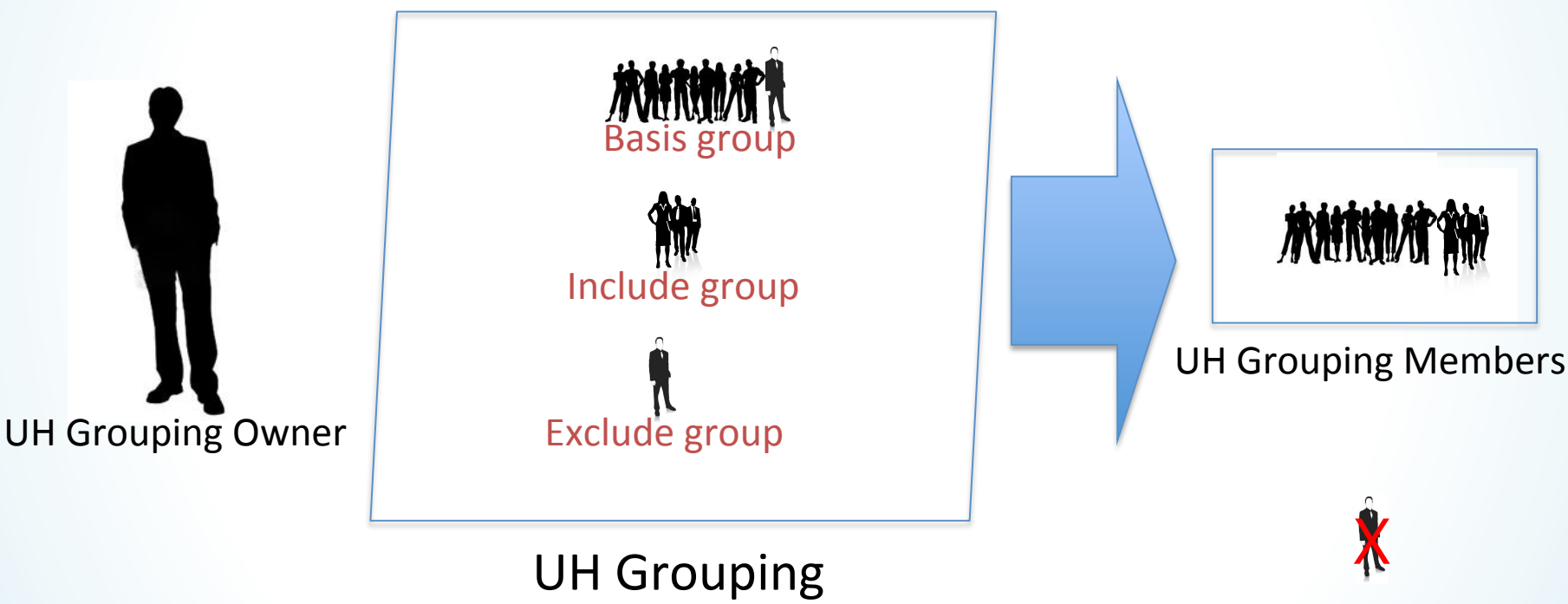
UH Groupings

- Ideas recently discussed:
  - UH App Developers: discussion list
  - UH App Developers: CAS3, Special DNs, Groupings
  - UHH ‘Ohana
  - UHM Executive-Managerial
  - Groupings for all UHIMS managed LISTSERV lists
  - ITC by floor mailing lists
  - UHIMC users (dual use: for authorization and email)

UH Groupings vs. Groups

- Grouper Groups vs. UH Groupings?
  - A Grouper group is a simple list of people.
  - A UH Grouping is a very flexible service.
    - User Interface for Owners and Members.
    - Automatic Groups for the Basis group
    - Membership tuning: Include/Exclude groups
    - Publication destinations
    - LISTSERV namespace reservations, whether you publish or not.

UH Groupings, Summarized



UH Groupings URLs

- UH Groupings online service:
  - https://www.hawaii.edu/its/uhgroupings
- Online documentation:
  - https://www.hawaii.edu/bwiki/display/UHIAM/UH+Groupings
- Requesting a Grouping, online form:
  - https://www.hawaii.edu/bwiki/display/UHIAM/UH+Grouping+Request+Form
- Developer documentation:
  - *Not yet available, stay tuned . . .*

Quick Tips & Reminders

Michael Hodges
Identity and Access Management Team Manager

Quick Tips

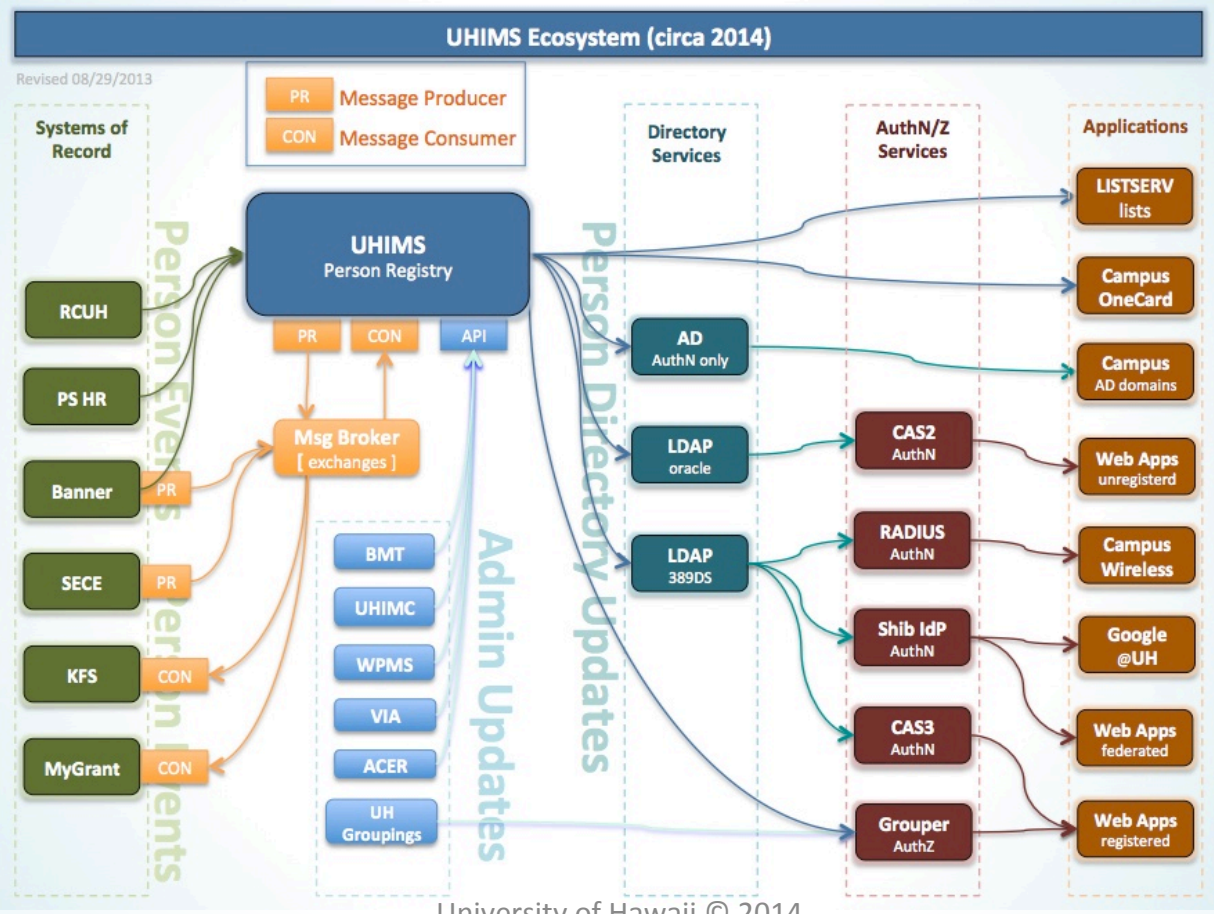
- VIA for Visitor Access to wireless networks
  - http://www.hawaii.edu/via/
  - Populates the LDAP misc branch, which means that the Web Login Service (CAS3) also authenticates VIA accounts successfully.
  - VIA is useful for providing 3rd party access to UH applications, assuming that the application is not also checking roles (student, faculty, staff).
  - ⚠ Warning, email addresses longer than 19 characters are truncated, which can be confusing.

Quick Tips

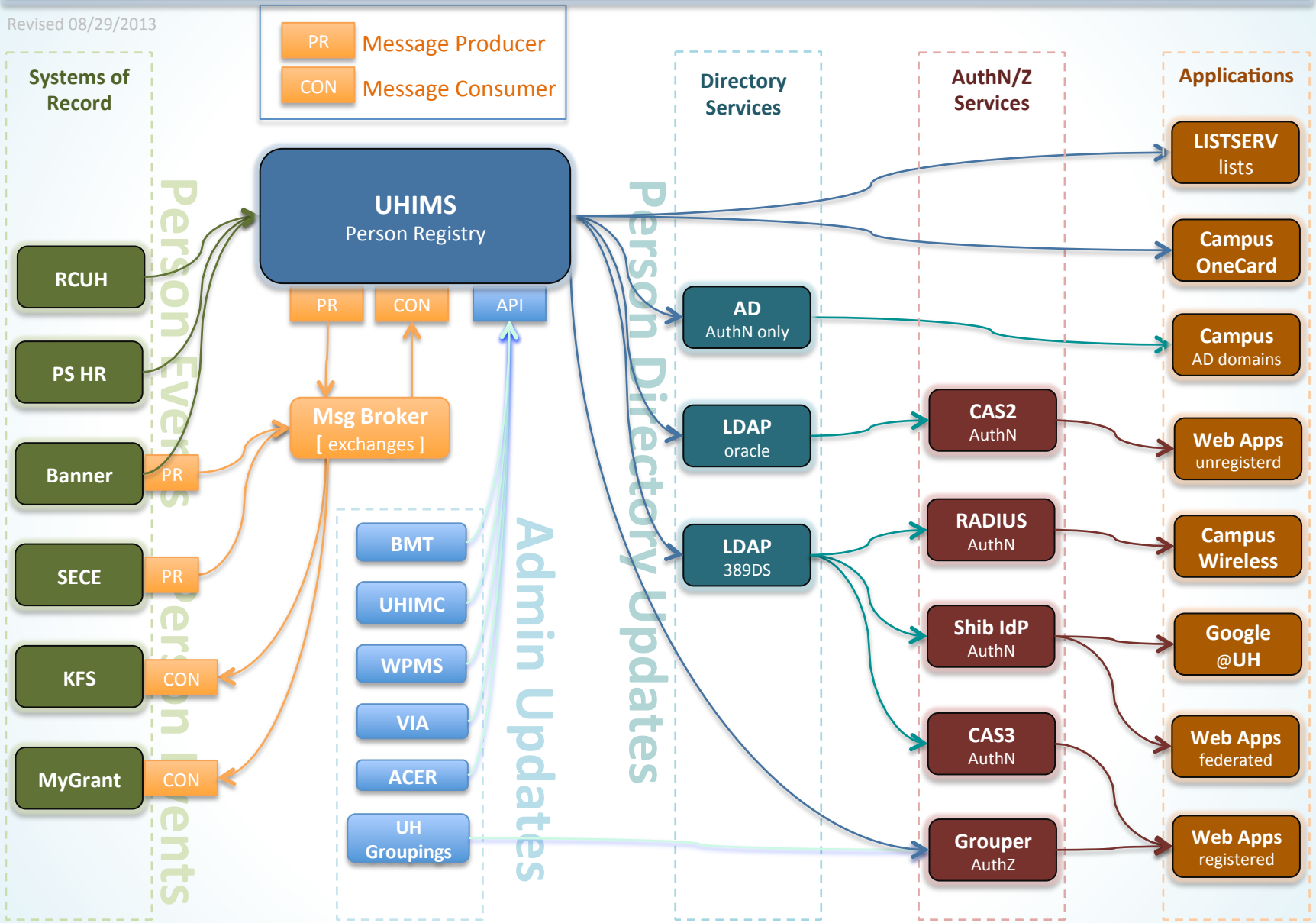
- UH Applications Developers LISTSERV List
  - Membership is over 180 and growing.
  - By default anyone requesting Special DNs, CAS3 or UH Groupings services is added.
  - The one list is shared by a broad range of IT staff and IT Managers.
  - Primary list communications include:
    - ITS IAM announcements for meetings and technical announcements for LDAP, CAS3, and UH Groupings.
    - Technical questions and IT information sharing within the UH IT community.

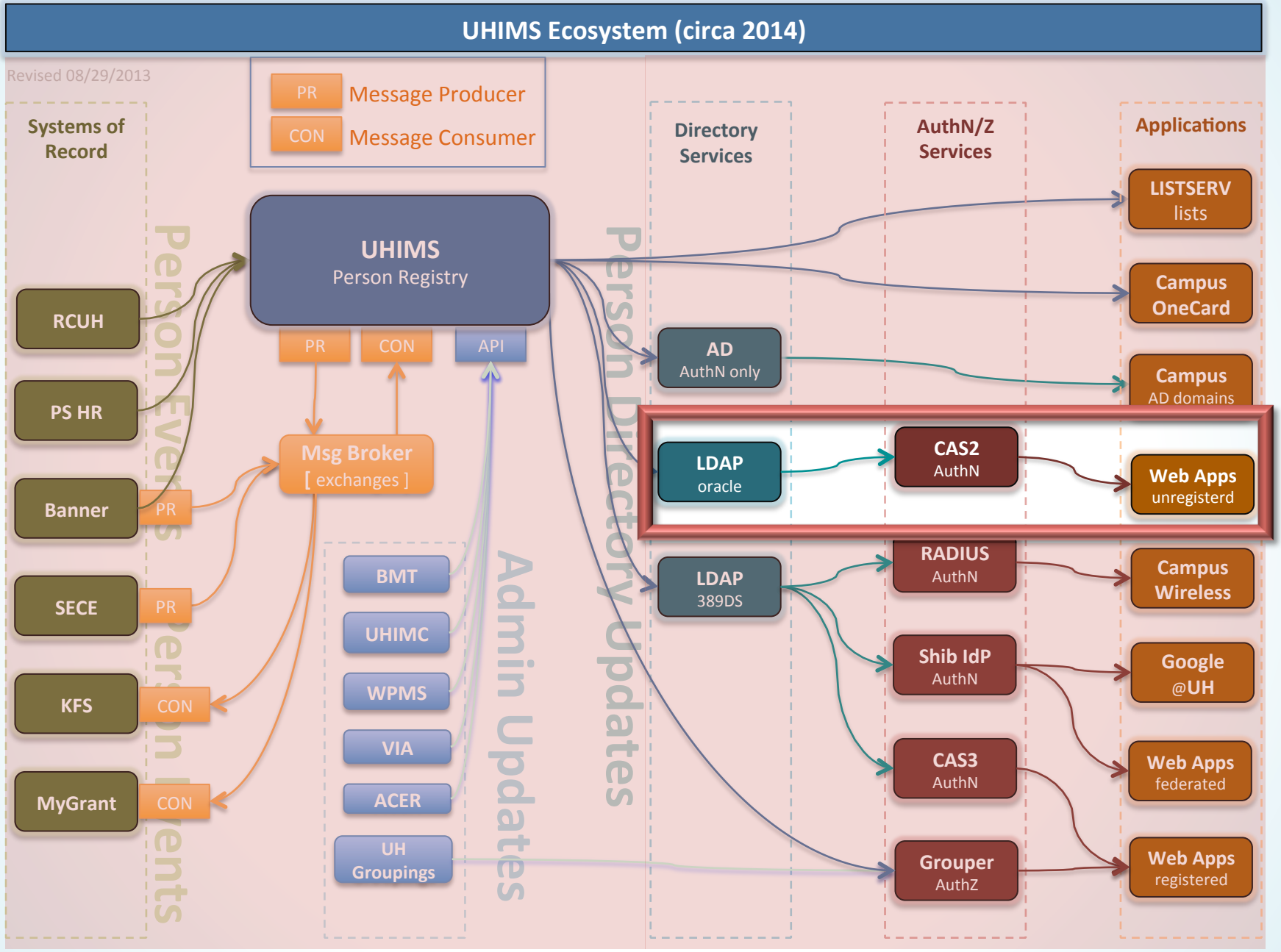
End of Service Life Reminders

- Legacy **CAS2** & **LDAP** – EOSL is **12/31/1014**



UHIMS Ecosystem (circa 2014)




UHIMS Ecosystem (circa 2014)
Revised 08/29/2013
PR Message Producer
CON Message Consumer
Systems of Record
Directory Services
AuthN/Z Services
Applications
UHIMS
Person Registry
PR
CON
API
RCUH
PS HR
Banner
SECE
KFS
MyGrant
Msg Broker
[exchanges]
BMT
UHIMC
WPMS
VIA
ACER
UH Groupings
AD
AuthN only
LDAP
oracle
LDAP
389DS
CAS2
AuthN
RADIUS
AuthN
Shib IdP
AuthN
CAS3
AuthN
Grouper
AuthZ
LISTSERV
lists
Campus
OneCard
Campus
AD domains
Web Apps
unregisterd
Campus
Wireless
Google
@UH
Web Apps
federated
Web Apps
registered
Person Events
Admin Updates
Person Directory Updates

Questions?

Note that we have attempted to capture the questions & answers and will publish what we've caught along with these slides.

https://www.hawaii.edu/bwiki/display/UHIAM/UH+Applications+Developers+forum

Wrapping Up

- Thank you!!!
- Hope you are enjoying the new ITC facilities.
- Snacks in the back
- Take a moment to introduce yourself to your colleagues (meet at least 1 new person)