THE UNIVERSITY
of
WISCONSIN
MADISON

IDM SOFTWARE: STRATEGIES FOR CHOOSING SUITES

June 22, 2011

Steve Devoti, Senior IT Architect, UW-Madison

UW-Madison

- Approx. 250,000 accounts
- 40,000 students, 14,000 fac/staff
- PeopleSoft
- We run much of the federated IAM for UW-System

The four disclaimers

- This presentation has been painstakingly researched, really it has.
- Collective bargaining? I don't need no stinking collective bargaining.
- Employees of the University of Wisconsin-Madison are lucky to be working at all (according to Gov. Walker) let alone taking up the valuable time of a Sr. IT Architect with questions they could have asked at the office.
- All opinions expressed here are well-reasoned and insightful. Needless to say, they are not those of the UW-Madison, InCommon, Internet2, Educause etc.

Level set

- Directory (i.e. LDAP)
- Provisioning (i.e. “IdM”)
- Web Access Management (WAM)
- Federation
- eSSO
- Entitlement (i.e. role management)
- Identity Audit
- Virtual directory

So you think you want an IAM Suite

Why? What are good reasons for considering a suite?

Cost

- Seems reasonable, buying a suite of solutions from a single vendor likely means you'll get a better deal.

However…

- They make it up over the life of the solutions through
  - License fees
  - Consulting
- Do no be under the illusion that you can just fiddle around with the extra pieces and deploy them yourself
- “Free” might not only cost you a lot of money, but sets the expectation that you will use something that really doesn’t meet your needs.

Effortless integration of IAM solution elements

- Seems reasonable, elements from a single vendor should be easier to integrate than those from different vendors.

WTF?

- History. With 1 exception (we'll discuss later) vendors have created these suites by acquisition.
- And… have done a HORRIBLE job integrating them.
  - Different UI's
  - Different policy stores (this is big)
  - Different approaches to APIs
  - Different approaches to standards
- I personally, am very, very disappointed.

Effortless integration with stuff like ERP

- □ Also seems reasonable, that for example the provisioning connector from Oracle’s IAM suite would work easily with PeopleSoft.

Why?

- Experts say customers expect this to work
- I'd say I expect the different part of the IAM suite to work together too. Oh well.
- I speculate that it is far easier to make IAM work with applications than other IAM.

Take a ways….

- There is little value in going with a suite
- "Best of breed" for each solution will likely be just as easy to integrate as a suite
- **IF** you **carefully** evaluate each solution in a suite and they will meet your needs, it could be a good deal

Options: Directory

- Active Directory, eDirectory, Red Hat, Open Directory, Oracle Internet Directory, CA, Sun Java (Oracle), IBM Tivoli, OpenLDAP ………
- RACF, ACF2
- It doesn’t really matter. This is the one area where vendors have high compliance with standards (and LDAP is simple)
- Look for low cost and good architecture fit.
- …or what you already have.

Options: Provisioning

- **Major Brands:** BMC, CA, HP, IBM, Microsoft, Novell, Oracle, SAP, Siemens
- **Regional or Specialty:** Beta Systems, Courian, Evidian, Fischer Intl., Sentillion, Hitachi ID
- **Boutique:** Avatier, Llex, iSM, OpenIAM, Omada, Volker

Options: Web Access Management

- Pretty much all the major brands
- CAS, PubCookie, OpenSSO
- Shibboleth
  - Don't fight it
  - Lacks some fancy features like delegation and web UI
  - But, we all use it. Built in support for federation, and coming soon, uApprove. Can support non-web clients via Extended Client Protocol (ECP).

Options: Federation

- Look for a WAM that natively supports SAML
  - This will meet the vast majority of needs
- However, if you need more:
  - Active Directory Federation, OpenID support, integration with certificates or OTP
- All the major vendors have solutions, but you may also want to check out:
  - Ping Identity and RSA

Other Stuff

- eSSO: ActivIdentity, Avatier, CA, Citrix, Evidian, IBM, Imprivata, Novell, Oracle, Passlogix, Quest….
- Entitlement (i.e. role management): The usual suspects, and Bayshore Networks, Axiomatics, BiTKOO, Jericho Systems, NextLabs, ObjectSecurity
  - Maybe overkill. A provisioning system, directory and group management may do it (Grouper, Quest)
- Identity Audit: Many/most already mentioned
- Virtual directory

Now what?

- Focus on the core, directory, WAM and provisioning
- RFP, RFI or POC?
  - If you have to do an RFP, go ahead. If not, don't waste your time.
  - Focus on good use cases and implementing a POC environment that matches production as closely as possible.
  - Use cases should "sliver", i.e. don't try to cover every scenario, but focus on scenarios that require interactions with as many elements as possible.

POC

- Takes time. A week is not nearly enough.
- You are not just evaluating the solution(s) you are evaluating the consultants. If They don't seem like they know what they're doing in the POC, well… in the real implementation…
- Consulting co. are starting to support open source (e.g. Unicon)

Random thoughts on success

- Stakeholder engagement (w/ a few exceptions) is overrated. This is infrastructure.
- These systems are COMPLICATED! Good consulting services are critical.
  - Review resumes.
  - DEMAND that once you settle on individuals, those are the ones you will get.
  - Buy local if you can.
  - Get over you're Midwestern/Southern politeness. If someone isn't performing, say so and put them in a cab to the airport.

A few words about Microsoft

- Microsoft has been behind the curve in IAM, especially in support for standards, however:
  - Their stuff does work together, developed in-house, and is of high quality
  - They own the desktop, where users authenticate perform password resets, etc.
  - Partners provide high quality solutions to extend capabilities
- Especially if you run a lot of MS (e.g. Exchange, SharePoint, Active Directory)
- Local, local, local, could save you big $$$

Me

devoti@wisc.edu