Identity Management in Heterogeneous System Landscapes: the SAP Solution

- Meta
  - time
    - Sep. 14th, 2006
    - 8AM PST
  - People
    - Larry Justice
      - Lead SAP US Security Consulting
        - Professional Services
        - Wants to change title to "SAP Player"
    - Gerlinde Zibulski
      - NetWeaver Product Manager Voice & Security
  - Whiteboard
    - http://services.sap.com/securitypartners
      - LDAP
  - Dude behind me sees MindManager and writes down what it is to try it out later
- Larry's intro
  - the job
    - internal urging to have specialized security group
    - they've made it!
    - now he has 9-ish direct reports
  - "English is a second language for me too, 'cause I'm a Texan."
- Decentralized User Maintenance
  - "but that as the old days"
  - Each SAP system [and others]
    - had their own login
    - user store
  - go to some customers
    - same person will have different username/passwords
    - don't make sense to me
      - "confused the holy be-jebus out of me"
    - but people do it.
- this guy rules
  - he is real
  - he says Nazis
  - he also makes fun of the new directory logo
    - it's a bunch of nodes connected together
    - "what is that thing? it looks like something that MSFT or the department of energy would be interested in."
    - "I remember when it was a little can."
  - "yesterday we had a union mouse: it would work, but it was really slow."
  - "I visit HR people and they have the [org-chart] setup entirely different than the real structure of the company. But, I guess HR people live in their own world."
  - "You here the LDAP guys say DIT this and DIT that. It's not Morse code, it's Directory Information Tree."
  - "...and I don't mind FI guys, as long as they sit at the other end of the table...when we're out"
  - theory of frequent company re-orgs
    - someone has a weird brother in printing who needs the business
    - so, you re-org the company and send them the business of printing new cards every qtr
- Central User Administration
  - CUA
  - as of 4.6C
  - CUA clients
  - CUA server
  - mo' problems
    - RFC people are changing passwords for connections
    - then this screws up the CUA client/server connection
    - and people usually go to the security folks when they need to go to the RFC folks.
  - LDAP synchronization
- SAP NetWeaver Portal with User Management Engine (UME)
  - Runs in JEE
    - no ABAP
  - FAQ
    - UME will not replace the CUA
    - Not extra admin
    - Anywhere you've got the UME, you really, really want to point it to one place
      - Use ACLs
  - With no directory
    - Working with Java security without the directory
    - propeller heads and their XML
  - With LDAP
    - see more and more people with a corporate LDAP
    - or people who just want to use LDAP
    - "we see that a lot"
    - we get the dangling of carrot of provisioning for the first time
      - "that's cool stuff. that's exciting stuff"
      - "and it's going to become more important to us in the world of services"
        - declarative
          - "den-pro" body allows us to have type of...?
        - programatic
          - Sounds like Java security
          - security over running code
  - Dual-spec portal
    - SAP ABAP
    - JEE Engine
    - Release as of SAP 2000 something
  - HR Data Replication
    - With 4.70 HR can replicate to LDAP
- Integrated User Management
  - LDAP was cool technology
    - But marketing people couldn't figure out lies to tell about it
    - So it just hung out in geek-land
  - Overview of IdM platforms
    - Or "Meta-directory" tool
      - virtual/federated directory
    - except the view is slanted by focusing on LDAP
    - [the bwhichard comment about "most people think LDAP==IdM"]
  - A lot of people raise their hands about using LDAP
  - says how LDAP admins don't want to add things at the root directory
    - My asumption: SAP wants to add stuff at the root
    - but the meta-directory can fake out SAP
- Setting things up
  - creating ALE communications user
  - cleaning up
    - getting SAP-land security inline with using directory
    - setting up LDAP
- LDAP setup
  - Information Model
    - DIT
  - SAP Schema extension
    - top,person,orgPerson,SAPaddonUM
    - e.g. entry
      - cn=D505050;O=SAP-AG;C=DE
      - ...more fields in slide
    - something about "mapper"
- LDAP synch from CUA pipes to
- NetWeaver Portal - Identity Management
  - features
    - Self-registration
    - Password management
    - LDAP directory
      - SAP or database as store
  - User Administration
    - Create, Copy, Modify, Search for users
    - Assign users to roles or place them in groups
      - Larry likes putting people in groups so that you can only change roles that the group has instead of visiting every user
      - b/c there isn't a mass-edit for user roles
    - account activation
      - approve/deny self-registered users
    - user history
    - the usual user mgmt functionality
    - ...more in slides
- Architectural Overview
  - Overview
    - You want to centralize all your user data
    - Apps accessing User Management
      - SAP NetWeaver Portal
      - Other J2EE Application(s)
    - User Management Core Layer
      - SPML
    - ...more in slides
  - Data Source Configuration
    - Type-based partitioning
      - Principals stored in diff places by type
      - users in LDAP
      - groups in DB
      - [assumably, the managemablty and frequency of mgmt drives decision.]
    - Principal-Based Data Partitioning
      - Principals of same type stored in diff data sources
    - Attribute-Based Data Partitioning
- LDAP connector
  - Something in SAP App Server needs LDAP call
  - Calls LDAP_RFC
    - since 4.6A
  - loads LDAP library
  - makes LDAP call to directory
- Demo
  - [Very PATROL-y in feel]
- Risk and Compliance Management
  - DirX works with GRC/Virsa
  - In role of creating a user
    - Access Enforcer does "cross-check" risk analysis
- Extending into the Enterprise
  - Meta-directory is exciting
  - Now we're services
    - [So, you extend more into and pull more from rest of enterprise.]
- IdM in a Heterogeneous World: Siemens Case - DirX
  - And now for a word from our partner
  - Siemens has the largest portal impl right now
  - Provisioning includes SPML
  - audit info
  - DirX Identity
  - DirX Directory
  - Siemens HiPath Slcurity DirX and DirX Identity
    - [They have some spelling problems]
  - Compliance Boost
    - no longer the red-headed step-child
      - "All we have to do now is use that one word SOX" to get people to listen
    - audit trail example with email
  - Simens IdM life-cycle slide
- Demo Pod Talk
  - SAP doesn't declare who primary partners are
    - [but Siemens shows up frequently]
  - Don't see Sun IdM too much
  - Standards/APIs/Interfaces
    - SPML
    - SAML
    - Liberty
    - WS-*
    - ["if it's in stock, we've got it."]
  - MDM tie-in
    - Architecturally, still separate.
    - [That is, it's concept-ware.]
  - Auditing/Governance
    - activities associated with identities in the system
- Questions
  - How does this IdM help with people moving from geo to geo?
    - e.g.
      - If I move from Asia to Texas
        - do I have the same ID?
    - [You need to code stuff.]
    - Physical security tie-in
      - Cards working across geos
      - GRC guys are woking on it for the door system
      - "that's awesome"
  - How does this tie into Shai's keynote?
    - Tying into MDM
    - [I think the question is: this seems like another data store instead of getting it into MDM.]
    - Answer
      - hrm...
      - "you're not really going to use MDM as your user repository. It's too grandiose."
      - ...maybe they'll get there one day.

www.RedMonk.com/cote/ | 2006
BY:
http://creativecommons.org/licenses/by-nc-sa/1.0/