Identity & Access Management

- Identity Management
- Access Management and
- The Monitoring, Auditing and Reporting for Compliance
Identity Management

So What’s The Problem Anyway?
Identity Management

How big is the Problem?

- Number of systems and applications
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
- Dynamics of the organization, systems, applications and users
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
- Dynamics of the organization, systems, applications and users
  - Size
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
- Dynamics of the organization, systems, applications and users
  - Size
  - Complexity
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
- Dynamics of the organization, systems, applications and users
  - Size
  - Complexity
  - Dispersion, decentralization, delegation
Identity Management

How big is the Problem?

- Number of systems and applications
- Homogeneous or Heterogeneous
- Number of users
- Dynamics of the organization, systems, applications and users
  - Size
  - Complexity
  - Dispersion, decentralization, delegation
  - Growth or volatility
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets
- Amount of Administrator time being spent managing user access
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets
- Amount of Administrator time being spent managing user access
- Complexity and cost of cross training Administrators
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets
- Amount of Administrator time being spent managing user access
- Complexity and cost of cross training Administrators
- Business Processes for:
  - Adding new users and granting access
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets
- Amount of Administrator time being spent managing user access
- Complexity and cost of cross training Administrators
- Business Processes for:
  - Adding new users and granting access
  - Changes to access rights
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets

- Amount of Administrator time being spent managing user access

- Complexity and cost of cross training Administrators

- Business Processes for:
  - Adding new users and granting access
  - Changes to access rights
  - Suspending/restoring access rights
Identity Management

How big is the Problem – continued

- Number and growth of calls to your help desk for password resets and account lockout resets

- Amount of Administrator time being spent managing user access

- Complexity and cost of cross training Administrators

- Business Processes for:
  - Adding new users and granting access
  - Changes to access rights
  - Suspending/restoring access rights
  - Deletion of access rights
Manual Provisioning

Organizations use slow and inconsistent processes to provision user access rights.

- Elapsed turn-on time: up to 12 days per user
- Account turn-off performance: 30-60% of accounts are invalid
- 1 FTE user admin only handles 300-500 users

User Change

Request for Access Generated

Users with Accounts

Policy & Role Examined

Approval Routing

IT InBox

Administrators Create Accounts
Identity Management

Options
Identity Management

Options

- Do nothing, status quo
  - Number and complexity of systems, applications, etc. are growing
Identity Management

Options

- Do nothing, status quo
  - Number and complexity of systems, applications, etc. are growing
  - Number of users is growing – internal as well as external
Identity Management

Options

- Do nothing, status quo
  - Number and complexity of systems, applications, etc. are growing
  - Number of users is growing – internal as well as external
  - Business requirements are increasing and increasing at an increasing rate
Identity Management

Options

- Do nothing, status quo
  - Number and complexity of systems, applications, etc. are growing
  - Number of users is growing – internal as well as external
  - Business requirements are increasing and increasing at an increasing rate
  - Increasing calls to the helpdesk and increased Administrators’ time
Identity Management

Options

- Do nothing, status quo
  - Number and complexity of systems, applications, etc. are growing
  - Number of users is growing – internal as well as external
  - Business requirements are increasing and increasing at an increasing rate
  - Increasing calls to the helpdesk and increased Administrators’ time
  - Requires additional IT resources
Identity Management

**Options**

- Homogeneous solutions
  - Microsoft
    - Works well if you are only a Microsoft “shop”
  - Novell
    - Works well if you are a Novell “shop” and do not have complex Identity Management and Security Requirements
  - Not much else
Identity Management

Options

- Heterogeneous solutions
  - Single Sign-On Solutions
  - Centralized Authentication to a LDAP directory
  - Federated Identity Management
  - Variety of vendors with solutions offering a range of functions, features and capabilities from limited to extensive
    - You get what you pay for!
Identity Management
Strategies and Approaches
Identity Management

Strategies and Approaches

- Do nothing, status quo
  - Works well if:
    - Number and complexity of systems, applications, etc. are not growing and are homogeneous
Identity Management
Strategies and Approaches

- Do nothing, status quo
  - **Works well if:**
    - Number and complexity of systems, applications, etc. are not growing and are homogeneous
    - Number of users is not growing – internal as well as external
Identity Management

Strategies and Approaches

- Do nothing, status quo
  - *Works well if:*
    - Number and complexity of systems, applications, etc. are not growing and are homogeneous
    - Number of users is not growing – internal as well as external
    - Business requirements are not increasing, or if
Identity Management

Strategies and Approaches

- Do nothing, status quo

  *Works well if:*

  - Number and complexity of systems, applications, etc. are not growing and are homogeneous
  - Number of users is not growing – internal as well as external
  - Business requirements are not increasing, or if
  - Additional IT resources are not a problem and are available
Identity Management

Strategies and Approaches

- Homogeneous
  - Microsoft’s Users and Computers console to manage users
  - Microsoft SPNEGO and Kerberos for Single Sign-On
  - Novell e-Dir
Identity Management

Strategies and Approaches

- Heterogeneous
  - Single Sign-On Solutions
    - IBM’s Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO)
Identity Management
Strategies and Approaches

- Heterogeneous
  - Single Sign-On Solutions
    - IBM’s Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO)
  - Centralized Authentication to a LDAP directory
    - Supported by all UNIX and LINUX O/S and some applications
    - Supported by most Web Application Servers and Portals
Identity Management

Strategies and Approaches

- Heterogeneous
  - Single Sign-On Solutions
    - IBM’s Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO)
  - Centralized Authentication to a LDAP directory
    - Supported by all UNIX and LINUX O/S and some applications
    - Supported by most Web Application Servers and Portals
  - Federation
    - Concept of ID Providers and Service Providers
    - Three protocols:
      - SAML, Liberty and WS Federation
    - Requires a Trust Agreement amongst partners for each to manage their own users and to define the protocol, version and content of the tokens
Identity Management

Strategies and Approaches – continued

- Implement an Identity Management (IDM) Solution
  - Variety of vendors with Identity Management or Account Provisioning solutions that offer a range of functions, features and capabilities from limited to extensive
Identity Management

Strategies and Approaches – continued

- Implement an Identity Management (IDM) Solution
  - Variety of vendors with Identity Management or Account Provisioning solutions that offer a range of functions, features and capabilities from limited to extensive
  - Independent Analysts provide insight and evaluations
    - Gartner
    - Meta
Identity Management

Strategies and Approaches – continued

• Implement an Identity Management (IDM) Solution
  ▸ Variety of vendors with Identity Management or Account Provisioning solutions that offer a range of functions, features and capabilities from limited to extensive
  ▸ Independent Analysts provide insight and evaluations
    • Gartner
    • Meta
  ▸ Keep in mind that there are three parts to this
    • Identity Management
    • Access Management and
    • the Monitoring, Auditing and Reporting for Compliance
Analyst View: Gartner on TIM

Strategic Quadrant Chart for GOAL vs. Viability

This Strategic Quadrant Graph is a reliable and well-informed starting point for evaluating specific vendor selection scenarios, and is from a Gartner Research Magic Quadrant.
METAspectrum: User provisioning

- Leader
- Challenger
- Follower

Performance vs Presence graph showing various companies' positions.

© 2005 META Group, +61 2 9290 0688, metagroup.com

© 2007 IBM Corporation

NSHE – IBM: Identity and Access Management
Identity Management

Next Steps
Identity Management

Next Steps

- Understand, define and document your environment, business needs and processes
  - Buyer’s Guide and Redbooks can help you with this task

- Perform a ROI analysis to determine if it is cost-effective
  - Use IBM’s ROI Tool to help you assess and calculate the ROI:

- Create and send out a RFI to determine which vendors can meet (or exceed) your requirements
  - Use IBM’s Identity Management Buyer’s Guide to help you with this task
Identity Management

Next Steps

- Understand, define and document your environment, business needs and processes
  - Buyer’s Guide and Redbooks can help you with this task

- Perform a ROI analysis to determine if it is cost effective
  - Use IBM’s ROI Tool to help you assess and calculate the ROI:
  - Or, create your own ROI analysis:
    - [ITIM Value Calculator.xls](#)
Identity Management

Next Steps

- Understand, define and document your environment, business needs and processes
  - Buyer’s Guide and Redbooks can help you with this task

- Perform a ROI analysis to determine if it is cost effective
  - Use IBM’s ROI Tool to help you assess and calculate the ROI:
    IBM Business Value Analyst Tool
  - Or, create your own ROI analysis:
    ITIM Value Calculator.xls

- Create and send out a RFI to determine which vendors can meet (or exceed) your requirements
  - Use IBM’s Identity Management Buyer’s Guide to help you with this task
    Tivoli Identity Manager Buyer's Guide
Identity Management

Next Steps

- Ask vendors to demo of their IAM solutions
- Participate in a hands on PoT to learn first hand about the IAM solution feature, functions and capabilities
  - Not all vendors provide this learning opportunity
- Invest in a Pilot – NOT a PoC!
Complex Organization:

- Numerous Distinct Business Units: SCHOOL OF MEDICINE, SCHOOL OF DENTISTRY, SCHOOL OF PHARMACY, SCHOOL OF NURSING, MEDICAL CENTER, CHANCELLOR'S IMMEDIATE OFFICE, VC-ADMINISTRATION & FINANCE, VC-UNIV ADVANCEMENT & PLANNING, CHANCELLOR-CAMPUSWIDE ACCTS, EXECUTIVE VICE CHANCELLOR, UNIV OF CAL FOUNDATION, NON-UNIVERSITY TENANTS, MC2-MEDICAL CENTER (CONTROL PT)
- Separate Authoritative Identity Sources for Each Business Unit

Identity Management Challenges:

- Integrate With Multiple Authoritative Identity Sources.
- Satisfy Discrete Requirements of Business Units while providing Interoperation

IBM Tivoli Benefits That Will Lead to an ROI

- Solution to multiple Authoritative Identity Sources – TDI Identity Feed System
- Standardized password policy enforcement
- Centralized and secure password store & maintenance
- Automated provisioning for basic account services (e.g. email, wireless, etc.)
- Improved compliance and security by quickly eliminating user accounts (de-provisioning)
- Reduced sign-on (improved user experience)
- Simplified security policy implementation across resources (improved security and lower administrative costs)
- Centralized auditing (improved compliance)
Access Management System

Identity Feed System:
Reads from Multiple Authoritative Sources to Create Credentials for Shared Identity Store: System of Record

Multiple Authoritative Sources for Each Business Unit:
- hr system
- Student registration System
- Contractors – visiting nurses etc.

Directory Integrator

System of Record:
DB2(MVS)

Identity Management System

Targets
- TAM LDAP(Solaris)
- Custom Applications
- AD (Win 2003)
- IBM IDS (AIX 5.3)

Identity Manager

J2EE / .NET
Web Applications
- Wireless Servers
- Web Portal
- Reporting Applications
- HR Applications
## Tivoli’s IT Operational Management Products: Strong Foundations for Administrative and Academic Computing

<table>
<thead>
<tr>
<th>Business Application Management</th>
<th>Server, Network &amp; Device Management</th>
<th>Storage Management</th>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Products include:</strong></td>
<td><strong>Products include:</strong></td>
<td><strong>Products include:</strong></td>
<td><strong>Products include:</strong></td>
</tr>
<tr>
<td>• Tivoli Composite Application Management</td>
<td>• Tivoli Enterprise Console</td>
<td>• Tivoli Storage Manager</td>
<td>• Tivoli Access Manager</td>
</tr>
<tr>
<td>• Tivoli Business Systems Manager</td>
<td>• Tivoli Monitoring</td>
<td>• Tivoli Continuous Data Protection for Files</td>
<td>• Tivoli Identity Manager</td>
</tr>
<tr>
<td>• Tivoli Intelligent Orchestrator</td>
<td>• Tivoli OMEGAMON</td>
<td>• TotalStorage Productivity Center</td>
<td>• Tivoli Federated Identity Manager</td>
</tr>
<tr>
<td>• Tivoli Service Level Advisor</td>
<td>• Tivoli NetView</td>
<td>• Netcool Monitors</td>
<td>• Tivoli Directory Server</td>
</tr>
<tr>
<td>• Tivoli License Manager</td>
<td>• Tivoli Remote Control</td>
<td></td>
<td>• Tivoli Directory Integrator</td>
</tr>
<tr>
<td>• Tivoli License Compliance Manager</td>
<td>• Tivoli Systems Automation</td>
<td></td>
<td>• Tivoli Security Compliance Manager</td>
</tr>
<tr>
<td>• Tivoli Monitoring</td>
<td>• Tivoli Workload Scheduler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tivoli Intelligent Orchestrator</td>
<td>• Tivoli Provisioning Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tivoli Service Level Advisor</td>
<td>• Tivoli Configuration Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tivoli License Manager</td>
<td>• Tivoli Decision Support for z/OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tivoli License Compliance Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Tivoli’s Netcool Products:

**Products include:**
- Omnibus
- Precision
- Real Time Active Dashboard
- TSOM
- Netcool Monitors
For More Information Contact:

David Crea
Phone: 1-425-820-2919
E-Mail: djcrea@us.ibm.com

Danya I Yaldoo
Phone: 1-415-545-2140
E-Mail: danyayal@us.ibm.com

J Alyn Ward
Phone: 1-425-831-0352
E-Mail: jalyn@us.ibm.com

Paul Wells
Phone: 1-916-224-6420
E-Mail: pcwells@us.ibm.com