ANALYSIS ON IDENTITY MANAGEMENT SYSTEMS WITH EXTENDED STATE-OF-THE-ART IDM TAXONOMY FACTORS

Madhan Kumar Srinivasan[1] and Paul Rodrigues[2]

[1]Education & Research, Infosys Technologies Limited, Mysore, India
madhan_srinivasan@infosys.com
[2]Department of IT, Hindustan University, Chennai, India
deanit@hindustanuniv.ac.in

ABSTRACT

Every person has his/her own identity. It's important to manage a digital identity in a computer network, with high priority. In spite of different applications we use in organization, resources need to be managed and allotted to the appropriate user with proper access rights. Identity management or IdM refers to how humans are identified, authorized and managed across computer networks. It covers issues such as how users are given an identity, the protection of that identity and the technologies supporting that protection. This paper attempts to provide an analysis to various identity management systems based on the state-of-the-art identity taxonomy factors.

KEYWORDS

Identity management, access management, digital identity, IdM taxonomies, identity management survey

1. INTRODUCTION

In the real world each and every person has his/her own identity. It is equally important to manage the identity in computer networks with high priority. Irrespective of different applications/platforms we use in organization, resources need to be managed and allotted to the appropriate identity/user (i.e. Provisioning Management) with proper access rights (Access/Policy Management). This process is called Identity Management. To achieve Identity Management efficiently the digital identity need to be defined properly.

Identity management refers to the process of managing the identities of users in providing privileges and access rights within a company or an organization by employing emerging technologies. There is a need for automated application, which defines what data and applications each user can access, to reduce the time in general. Identity management aims at increased security and productivity reducing the costs associated with management of user identities, attributes and their credential. Identity management uses a middleware tool that identifies the users and manages the privileges and access rights to resources. It minimizes the multiple user identities across various networks to a single identity that is accepted globally. Secure identity management touches many diverse capabilities like self-service, single sign-on, content aggregation etc.

2. RELATED TO THIS WORK

In this paper we are trying to extend our pervious survey [1] with some extended factors. When we think of assessing the IdM market, initially we faced two primary issues. The first issue was that on whom we are going to evaluate? And the second was, on what? By now the IdM market

DOI : 10.5121/ijasuc.2010.1406

is very vast with many vendors. And almost all of them are really doing the great job (at least on any one of the major functionality). By considering the mentioned fact we decided to depend on IdM related research organizations, in selecting vendors and evaluation factors.

2.1. Vendor Selection

As a continuation our previous work, in this paper also we are considering the same five different identity management vendors (from ~15 top IdM vendors). These vendors are finalized based on the research results of two identity management research groups. They are Burton Group [6] (www.burtongroup.com) and Forrester Research, Inc [10] (www.forrester.com). Forrester is being treated as one of the top research organization for independent technology and market research worldwide. And Burton Group is the leading research organization for IAM architecture and infrastructure related research. By considering various research reports by Forrester and Burton Group we are finalizing IBM, Novell, Sun, Oracle, and CA for this survey.

2.2. Survey Taxonomies

To measure the above selected IdM products we decided upon the following 2 classifications. With the base of these classifications, one can have a clear eye opener on any identity management tool. So we would like to represent these classifications as state-of-the-art identity management taxonomies. And these taxonomies are further categorized into ten sub-factors. They are,

1) Features & Capabilities

- Initial setup and system integration
- Data management
- Delegated administration and self-service
- Access management
- Policy and role management
- Architecture
- Customer references

2) Strategy & Vision

- Identity management vision
- Breadth of identity management solutions
- System integrator (SI) partnership

3. IDM SYSTEM REVIEWS

The reviews of selected IdMs are discussed here. After this section the results are compared and analyzed in the next section.

3.1. IBM Tivoli Identity Manager

IBM Tivoli Identity Manager (TIM) 5.0 version is being used for this survey. TIM uses custom agents that are installed on every managed resource, such as AD domain controllers, database servers, etc. IBM states [20] that many of its agents don't need to be installed on managed resources, but can manage multiple resources remotely from a single server.

Before TIM starts its activity, it must integrate some of the existing applications like client's directory, HR applications, etc. For this task, IBM uses TDI (Tivoli Directory Integrator), a Java application that functions as a junction of identity data, both for initial integration and as a permanent connector when needed. TDI can be installed on Windows & Linux platform. It helps the organization by offering a clear view of any managed resource. TDI assures the user with all integration tasks by providing easy methods to reformat dissimilar data, such as consistently formatting phone numbers, Social Security numbers, and birth dates, etc.

TIM's simulation feature is an advantage, which allows user to try policies like create approval steps, assign tasks, etc, before enabling them.

Paul Venezia [11] states that, the overall navigation of the UI wasn't so clear. He further states that when user tries to construct some action, they need to plug JavaScript code into (the small text field available) in the UI. This provides some power, but it's also significantly more complex and substantially less elegant than expected. Paul Venezia research describes that, the reporting engine of TIM is vast and complex. It's possible to generate reports containing nearly any data present in the system, but again, it's a little challenging to assemble the data in a logical form. Crystal Reports integration is also present in TIM.

3.2. Novell Identity Manager

Here we have used Novell's Identity Manager 3.6.1 version for this survey. Novell's identity management solution relies heavily on the company's directory server, eDirectory, which gives backbone support for all identity management activities. Novell's suite provides all identity management features including password management, role-based provisioning, cross-application user management, user deprovisioning, and corporate white pages functionality.

Identity Manager handles all IdM tasks with administrator-defined identity policies, by making communication between Identity Vault and the other applications on the network. All this depends on Identity Manager Drivers, which are the agents needed to manage all applications. Here communication between Vault, Drivers, and Identity Manager is totally based on XML.

Novell has an excellent UI, Designer. Designer proves the Novell solution as a masterpiece among others. But it's important to note that this is an optional add-on. Based on the Eclipse framework, Designer allows administrators to lay out almost the entire identity implementation visually and then drill down for configuration. Designer allows much of the configuration to be done in a simulated sandbox mode. The Designer is for policy management, workflow design and simulation, and documentation.

The only area where Novell uses outside tools is when we need to merge two different AD's. First it uses Microsoft AD tools to migrate and then uses Identity Manager to manage all the data through its Identity vault. From administration to reporting, Novell Identity Manager proves to be one of the easiest to-use solutions in the collection. The addition of Designer adds even more automatic functionality on top of this suite.

Novell's policy management and delegated administration are split into two applications — which can be an inconvenience in large deployments [11]. Novell fares well in several of the functional areas of assessment; although it establishes leadership [10] in the data management, auditing and reporting, and architecture criteria sets, it trails in delegated administration and self-service, as well as in policy and role management. The disadvantage is that the product is dependent on eDirectory, which is one of the factors contributing to a skills gap that organizations often face and a need to bridge when selecting Novell for IAM.

3.3. Sun Java System Identity Manager

In Sun Java System Identity Manager 8.0 we can find a level of reliability and maturity that's rare in other IdM products. Sun's entire identity management suite consists of Access Manager, Directory Server Enterprise Edition, Federation Manager, Identity Auditor, Identity Manager, and Identity Manager Service Provider Edition.

Comparing with other IdM products Sun's is completely agentless. Its technology is fully responsible for monitoring and interacting with existing directory servers and applications without the need to deploy agents. For certain technologies, such as AD or Novell's directory, Sun deploys a black-box style software gateway for data translation, but this is not an agent, nor does it require changes to target systems in order to function. In practice [11], this looks very efficient. Sun uses Web-based, wizard-driven configuration tool to configure all resources, rules, users, and everything else. When there is need to migrate one AD into another, Sun Identity Manager manages it without any use of Microsoft AD tools.

Sun’s provisioning capabilities are extremely flexible. All events in the product can trigger workflows, which helps Sun Identity Manager meet very demanding customer requirements with minimal customization. Forrester Research survey [10] points that, Sun’s Access Manager Solution is not up to the mark in the areas of centralized configuration management, policy definition, and adaptive authentication. Generally, the breadth of Sun’s IAM portfolio is short of competitors Oracle and IBM (lacking E-SSO, identity audit, privileged user management, and entitlement management), and Sun has not yet fully implemented its open source strategy across the board of IAM products. Sun needs to focus on enhancing ERP connector capabilities and integrating audit log management systems more tightly with its products. Although the talent pool on the market for Sun’s IAM skills is fairly rich, Sun has lost its exclusivity or elite status with SI partners, especially to Oracle.

3.4. Oracle Identity Management

Considering Oracle Corporation, we take its version of 11g for our analysis. In addition to Oracle Identity Manager (OIM) and Oracle Access Manager (OAM), its recent acquisition and integration of role management (Bridgestream/Oracle Role Manager [ORM]) and risk based authentication (Bharosa/Oracle Adaptive Access Manager [OAAM]) products will help Oracle position its IAM product set as the identity services foundation for all Oracle eBusiness products. In general Oracle’s identity management platform has excellent enterprise role management capabilities [7].

Functionality-rich connectors and a special staging area for intermediary data transformations allow for flexible data transformations. Oracle has retired all user management and workflow functionality features in OAM, and it plans to unify all such functionality, along with reporting and auditing, as a set of common services. The product directly supports rollback functions through Oracle’s Total Recall feature, in addition to having workflow-enabled connections to endpoints. There is a wide array of options for detecting and dealing with orphaned accounts. Oracle’s provisioning policy definition supports wildcards and nested roles. OAM natively supports chainable and pluggable authentication schemes, flexible policy design, and native multifactor authentication using OAAM. Oracle licenses Passlogix’s E-SSO solution in an OEM agreement and integrates it with OIM for Windows-based password self-service.

ORM’s advanced temporal role versioning and native support for multidimensional organizations and OAAM’s easy-to-use multifactor and adaptive, risk-based authentication and fraud detection boost Oracle in front of the competition on functionality. Meanwhile, Oracle’s focus on extending IAM from a security and systems management discipline to one of application architecture and development fuels its strategic leadership.

3.5. CA Identity Manager

CA has its recent Identity Manager r12 version for this analysis. CA has a leading Web SSO product with SiteMinder, but its Identity Manager still carries the burden of the legacy CA Admin provisioning engine, while only supporting CA Directory for the global user store [10].

CA's adaptable SiteMinder shares policies with Identity Manager's Delegated Administration Functionality, SOA Security Manager (the service-oriented architecture access management system), and SiteMinder Federation. Identity Manager's administrative model currently provides preventive — but not detective or corrective — SoD management (Segregation of Duties), a missing feature that will be present in CA's forthcoming Security Compliance Manager.

Based on the survey of Andras Cser [10] and his team, CA needs to eliminate the dependency on the inheritance CA Admin and CA Directory. Currently CA offers the Enterprise Entitlement Manager as a optional add-on to its IAM suite. But most of the customer survey states that, CA's Enterprise Entitlement Manager needs to be integrated into IAM suite to remain competitive in the market. CA's SiteMinder is still a tough competitor for any Web SSO implementation. But, it is having a drawback in its ability to chain independent pluggable authentication modules — a foundation feature for adaptive authentication. Customer references expressed concerns around 1) the scalability of CA Identity Manager's policies for large deployments and 2) CA's continuing ability to support its IAM products, as they witnessed a decline in technical support engineers expertise level.

4. ANALYSIS OUTCOMES

This section describes the comparative study of all IdM systems discussed so for. Each and every graph representation carries the weightage values in Y axis for the mentioned feature. Y axis is evaluated for the values between 1 and 10. Here the lower bound starts at 1and it represents minimum weightage. Similarly the upper bound ends at 10 and it represents maximum weightage. The values mentioned here are calculated based on various factors and references. And at most all such references, including marketing research analysis, customer feedback, etc are specified at reference section. These values are calculated with reference to the availability of data at a specific time period. So, our results may vary/conflict with other survey/reports. But depending on those of our factors and analytical methodology, these outcomes can give a good insight to users about various IdM systems.

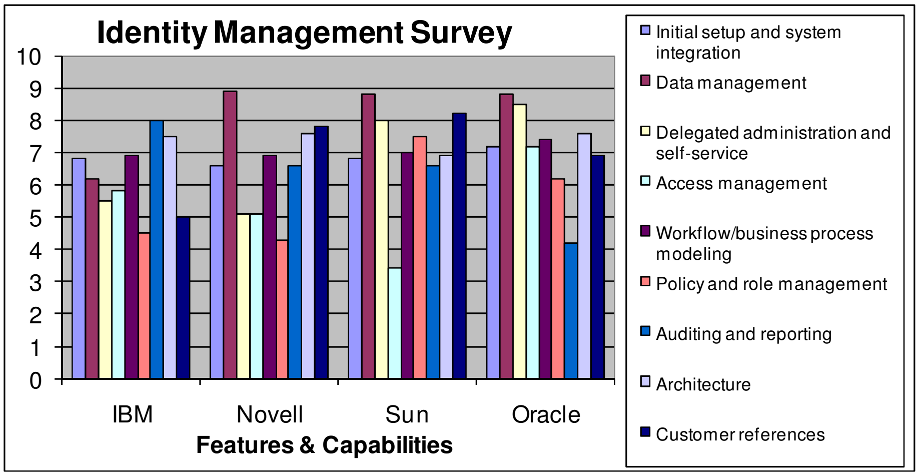

Figure 1. Comparison of IdM's on Features & Capabilities factors

The above figure describes the influence of each and every corner of Features & Capabilities taxonomies in various identity management products.

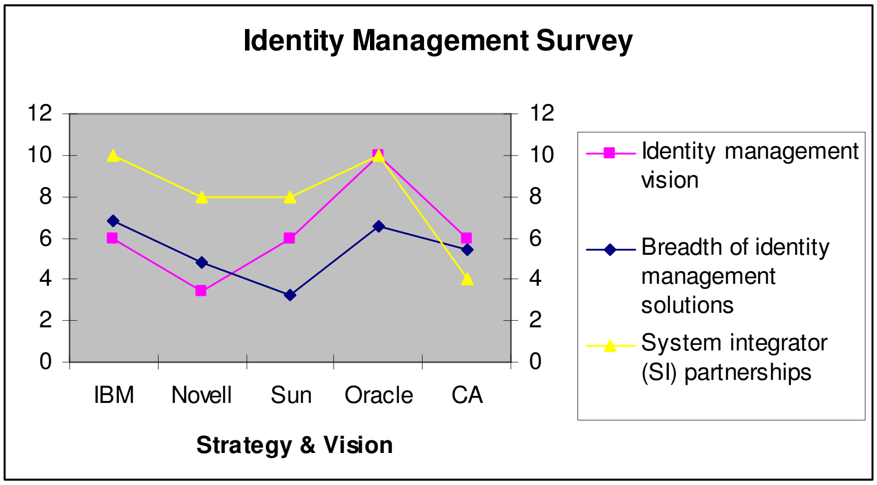

Figure 2. Comparison of IdM's on Strategy & Vision factors

With a clear perspective of first taxonomy, Figure 2, further describes the variations of Strategy & Vision taxonomies.

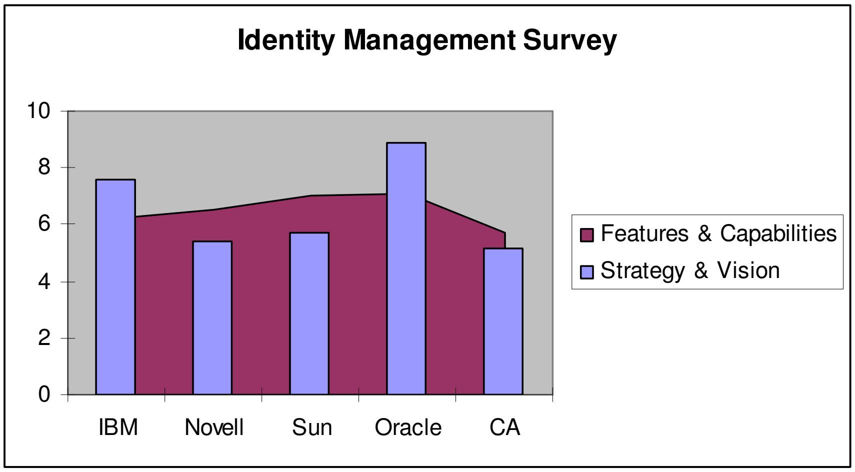

Figure 3. Individual level-wise analysis on two state-of-the art taxonomies

Figure 3 clearly shows the impact of various IdM products with respect to the state-of-the-art identity management taxonomies. In the figure Features & Capabilities represented by wave and Strategy & Vision is represented by bars.

3. Conclusions

As the IdM market is growing day by day, this enhanced survey can be helpful for both organization and user in attaining their requirements. This paper is an attempt to provide standard taxonomies in the area of identity and access management. Still there are many more taxonomies to be considered and excavate (can be our future scope). So, we are not concluding with the best or worst any more. Identity management has successfully influenced many IT and business industries because of its composite nature in both features and benefits. Even after years of healthy adoption rates, the IdM market is actually just beginning its path toward broad adoption and deep penetration.

References

[1] Madhan Kumar Srinivasan & Paul Rodrigues, “A roadmap for the comparison of identity management solutions based on state-of-the-art idm taxonomies”, Book on Recent Trends in Network Security and Applications, CCIS, pp. 349–358, Springer 2010.

[2] Philip J. Windley, “Digital Identity”, O’Reilly Media, Inc.

[3] Ruth Halperin & James Backhouse, “A roadmap for research on identity in the information society”, Identity in the information society journal volume 1 (1) paper no. 1, Identity Journal Limited, Springer 2008.

[4] Corinne S. Irwin & Dennis C. Taylor, “Identity, Credential, and Access Management at NASA, from Zachman to Attributes”, ACM, 2009.

[5] Dan Tynan, “Federation takes identity to the next level”.

[6] Lori Rowland and Gerry Gebel, “Provisioning Market 2009: Divide and Conquer”, Burton Group Market Insight Report 2009.

[7] Marc Chanliau, “Oracle Identity Management 11g”, An Oracle White Paper, February 2010.

[8] Eric Lai, “Novell to extend identity management to cloud, virtualized apps”, Dec 2009.

[9] Greg Nawrocki, “Open Source Identity Management and the Grid”.

[10] Andras Cser, “Identity and Access Management”, Forrester Research Report, 2008.

[11] Paul Venezia, “The identity management challenge”.

[12] Ehud Amiri, “CA IdentityManager: Capabilities and Architecture”, 2009.

[13] Chris Lavagnino, “Delivering Identity and Access Management as an Automated Service”, CA, 2009.

[14] John Fontana, “Novell, Sun, Oracle crank out identity management wares”.

[15] “Novell Identity Manager 3 Demo”, Novell Inc.

[16] “Novell Identity Manager Compare”, Novell Inc.

[17] “Oracle Identity Management 11g Datasheet”, Oracle Corporation.

[18] Deborah Volk, “Oracle Identity Manager 11g”, Identity Management Experts Series, Identigral, Inc, 2009.

[19] “Sun Identity Manager 8.0 Workflows, Forms, and Views”, Sun Microsystems, Inc, 2008.

[20] “IBM Tivoli Identity Manager Documentation”, IBM Corporation.

[21] Neil McAllister, “End-to-end identity management suites still coming together”.

[22] “Identity Management Market Forecast: 2007 to 2014”, Forrester Research Report, 2008.

[23] Burton Group Blogs, Identity and Privacy.

[24] Deborah Volk, “The rise of Suncle (volume 1)”, Identity Management Series, Identigral, Inc, 2009.

[25] Deborah Volk, “The rise of Suncle: Access Management”, Identity Management Series, Identigral, Inc, 2009.

[26] Deborah Volk, “The rise of Suncle: Directory Services”, Identity Management Series, Identigral, Inc, 2009.

Madhan Kumar Srinivasan

Madhan Kumar Srinivasan is a Member of Education & Research, Infosys Technologies, India and a Research Scholar of Hindustan University, India. He has received B.Tech in IT from Anna University, India and M.Tech in CSE with a CGPA of 9.05/10 from Dr.MGR University, India. He has published 11 (refereed) papers at both International and National levels, including IEEE & Springer publications. He has also served as a technical reviewer and chair for many conferences (IEEE, Springer and the like) around the globe. Also, he was an author of a chapter in the book “Recent Trends in Network Security & Applications” during July 2010 published by Springer Berlin Heidelberg publications, New York, USA. In addition, he is a designated reviewer for International Journal of Advances in Information Technology (JAIT, ISSN 1798-2340), Academy Publishers, Finland. He is an active member of many professional-bodies like Identity Research Group, International Association of Engineers, Computer Society of India & Teachers Academy, and has organized/contributed more than 30 events (conferences/workshops/symposia) in both International and National levels. His areas of expertise include Object Oriented Systems, Identity Management, Semantic Web, Network Security, etc. He is also a recipient of most prestigious ‘*Inspiring Teacher Award 2010’* from Teacher’s Academy at Osmania University, Hyderabad, India.

Paul Rodrigues

Paul Rodrigues is Dean IT, Hindustan University, India and CTO of WisdomTree Software Solutions, Chennai, India. He has received his B.Tech from Karnataka University, India & M.Tech from NIT-Allahabad, India and Ph.D from Pondicherry University, India. He has total 20 years of Teaching and Industry experience in Delivery Management, Software Engineering, Budget Management and Business Development. He has published more than 50 (refereed) papers in International Conferences/Journals which include Extreme Programming, Software Architecture, Databases and Object Oriented Analysis and Design. Also, he was an author of a chapter in the book "Recent Trends in Network Security & Applications" during July 2010 published by Springer Berlin Heidelberg publications, New York, USA. He is first in the world to apply Vastu to Software Architecture. He has worked in various domains that include Insurance, Retail, Digital Forensic, Content Management and Application Migrations. He is an active member of many professional-bodies like Identity Research Group, PMP, and CISSP.