Identity Management – White Paper

Harjeev Dhingra, Principal Security Architect, NetCom Systems Inc.

Overview:

This white paper discusses a set of recommendations and best practices methodology that facilitates the successful delivery of projects in the complex world of Identity Management solutions implementation.

The objective of this paper is to outline and discuss three essential elements that enable the effective delivery of an Identity Management solution in a client environment.

Introduction:

An Identity Management solution deployment often represents a company's first exposure to a project spanning the entire enterprise. Developing a consistent and effective Identity Management strategy requires a sound understanding of the approaches and technologies available for use to address multiple identities. Organizations need to implement both short term and strategic approaches to controlling identity.

Identity Management enables organizations to automate the management of identities, access rights, and resources across multiple IT applications and business processes. Given all the systems, applications, networks, domains, users, locations, etc., it would be easy to assume that a core capability of every Identity Management solution is simplified integration. Not true. The Identity market has evolved over the last decade and vendors' standard approach to creating identity products has been to develop and/or acquire various vertical applications. This requires investing inordinate amounts of time and resources integrating the disparate pieces, but do not enable simplified integration across enterprise systems. Without integration technology as the foundation, the solution does not span domains or enterprises, and is far too limited and expensive for a managed service environment. As a result, the client gets a very expensive and highly inefficient solution.

Provisioning systems (which create, edit, and delete accounts), virtual directories (which broker queries for identity data across disparate repositories), and metadirectories (which consolidate policy and management across identity systems) are a rich source of metrics because they typically contain critical metadata about identity definition, locale, and status. Identity can be a unique identifier in a virtual directory or metadirectory, a fact that drives several primitives.

At its simplest, identity provides the basis for access control, and therefore the quality of identity information forms the foundation for enterprise security architecture.

The rules, audit logs, filters, approvals, and delegations to which digital identities are subjected to, therefore become the chief informants to identity governance.

Benefits of Identity Management:

A well designed Identity Management Solution can provide significant benefits for organizations by improving, and more importantly securing access control to network resources. Typical benefits include:

Provisioning - Provides account request, validation, create, approval (workflow), propagation, notification capabilities.

Access Management - Provides authentication and authorization services with an ultimate objective to provide simplified sign-on.

Federated Identity Management - Represent products and standards that extend an authentication context to external parties.

Identity Unification - Represent Directory, Virtual Directory, and Meta-Directory offerings.

Top Identity Management Solution Goals:

Identity Management allows organizations to extend access to their information systems without compromising security. Organizations provide this extended access by precisely managing entitlements and modifying or terminating access rights promptly.

The following key deliverables are typically associated with Identity Management Solution:

Role and Policy Definition Non-Correlated Account Cleanup Design Workflow Process Federated Identity	High
Rule Based Access Control Access Dashboard Reporting Comprehensive Account Revocation Password Synchronization	Medium
Security via policy extn./enforcement Self Service Password Reset Help Desk Procedure Single Sign-On	Low

Please note that the deliverables are classified per level of difficulty rating measured in High, Medium and Low.

Identity Management – White Paper

Harjeev Dhingra, Principal Security Architect, NetCom Systems Inc.

Top 3 Drivers for a successful IM Solution:

Every organization has different business drivers for determining and implementing an Identity Management Solution. To ensure the greatest possible chance for success, strategy must align with business goals in order to drive business results.

1. Analyze existing access to various systems and consolidate them into Roles and Policies.

- Review existing access control lists across all the namespaces.
- Develop Roles and Policies.
- Import of Existing Roles from an Authoritative Source.
- Role vs. Actual Analysis.
- Rule Based Roles assignment.
- Associate Roles to Users.
- Alert all concerned parties of the change

2. Process employee related feeds coming from reliable sources like HR to update user records.

- Understand data formats used in HR data feeds
- Map HR Feed data attributes to the User attributes
- Ensure account data is correct and complete
- Push changes to multiple systems seeking Identity Data.

3. Implement Workflow/Approval process and Self Service portal.

- Design Workflow/Approval flow chart from beginning till the end
- Assign Manager/Business Approver to the respective users
- Handle account change requests (create, modify, revoke etc)
- Route change request to all concerned parties for approval

Case Study:

Industry :

A Fortune 100 company with primary business in Insurance and Financial Services.

Employees :

50,000+

Products Deployed :

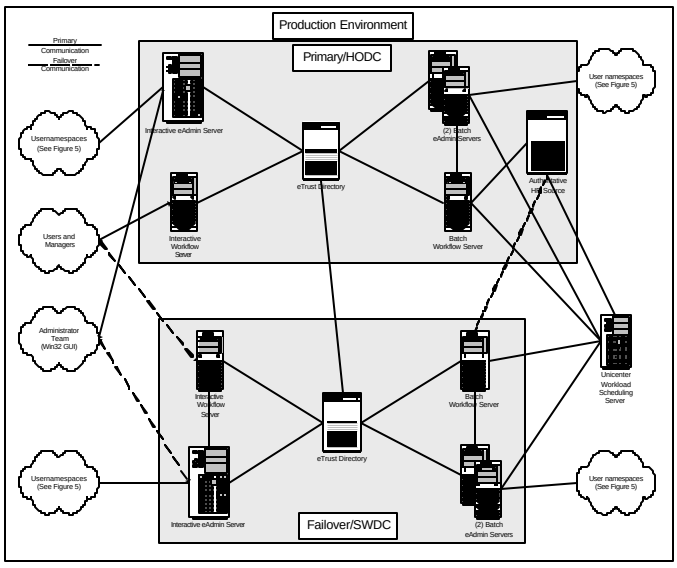
- eTrust Admin
- eTrust Access Control
- eTrust Audit

Architecture Overview :

The Client has two locations, a Primary and a Failover that hosts five Windows servers each. Each location has one interactive Admin Server, two batch Admin Servers, one interactive Workflow/Web Server, one batch Workflow/Web Server, and one Sun SPARC Server for the eTrust Directory Server.

A number of connectors were installed on the Admin Servers. Locations were linked by standard network hardware, providing communication via standard protocols. The primary Directory Server communicated with the secondary Directory Server, for data replication.

Unicenter System and Workload agents were installed on all the systems. TNG agents notified the TNG Event Manager of critical events, whereby the Event Manager triggered event-driven actions on certain systems.



Identity Management – White Paper

Harjeev Dhingra, Principal Security Architect, NetCom Systems Inc.

Business Benefits:

The following key business benefits were achieved by the client as a result of implementing the Identity Management Solution.

- Provision user on "Day One" of employment
- Efficient streamlined provisioning of user account across all business units
- Reduced overall time of user provisioning cycles by automating the process across multiple business units.
- User provisioning across various platforms and applications like MS Windows Active Directory, UNIX, AS400, Mainframe, Oracle Database and SAP.
- Access Monitoring and Audit

Implementation Details:

The implementation involved user provisioning of around 30,000 users across multiple systems. The project was divided into three phases. The first phase was implemented within 6 months. The system interoperated seamlessly with the following diverse platforms.

- OS/390 Top Secret
- Unix accounts (AIX, HP/UX, and Solaris)
- Windows 2000 Active Directory (including global group membership)
- Oracle
- DB2
- Exchange (5.5 and 2000)
- NT4.0 domain accounts (including global group membership)
- SAP profiles
- Entrust certificates
- DB2/UDB
- AS400

The Identity Management Solution provided client with the ability to effectively provision user accounts to new and existing employees in an automated fashion.

Conclusion:

Identity Management solution implementations can be a complex projects but they do not necessarily have to be expensive and disruptive. In fact, implementing an Identity Management Solution can be easily accomplished, provided the top three drivers presented in this paper have been identified and designed into the implementation process.

This solution can lead to recognizing other benefits including improved efficiency, secure confidential information, and integrity of financial information.

About NetCom Systems Inc.:

NetCom Systems Inc. is an Edison, NJ based Security and Network Integration consultancy firm. NetCom Systems has strategic partnerships with CA, Cisco Systems and IBM and provide high end technology solutions enabling greater ROI for clients deploying network connectivity and security solutions.

Based upon extensive experience in security and enterprise systems management NetCom Systems excels in delivering high quality assessment, design, implementations and managed information security solutions in the following areas:

- Security Consulting and Management
- Security Infrastructure Architecture and Implementation
- Managed services for IDS, VPN, FW, HIPS, NIPS,
- Enterprise Management Consulting and Implementation
- Content Security and Policy Enforcement
- IT Audits, Network & Risk Assessments
- Architecture consulting and Project Management
- Custom Development and Integrations

About the Author:

Harjeev Dhingra is a Principal Security Architect at NetCom Systems Inc. Harjeev has over 8 years of experience in designing and implementing security solutions for Fortune 500 clients. His core expertise is in areas of Identity and Access Management, Security Information Management, Compliance and eGovernance. Harjeev is a CISSP, CCNA, CUE, Tivoli Certified and has completed numerous certifications in security solutions from Cisco, CA and IBM.