Case Study
Retail Industry
Sage, TIM & TAM

Author:
Mark Funk, Trinity Solutions
Senior Tivoli Consultant, with over 25 years of extensive experience in the Information Technology Industry with a excellent technical background in supporting Enterprise Management, Security Compliancy, and E-business Disciplines, Tivoli Architecture/Automation, and Systems Management. His primary expertise focuses on Tivoli Management Framework, ITM, Monitoring for Databases, Messaging and Collaboration, Business Integration Manager, Tivoli Enterprise Console/NetView, Access Manager, and Identity Manager.

Project rationale

Audit motivation
Security was a significant issue from previous audits. Despite incremental improvements, auditors for TCP want better processes.

Additionally, as a publicly traded company, there are regulatory compliance motivations.

Business process improvement
Retail is a fiercely competitive business. Success depends on brilliant merchandising, creative marketing and intense cost control.

Solution requirements

The Children's Place needed a solution that would implement quickly and versatile enough to cover their heterogeneous IT environment. TCP also needed to address areas highlighted in audits that include regulatory compliance, inefficiencies in user management and policy formulation. A solution that will automate user provisioning processes which will result in less time being spent on creating and managing user accounts and centralizes provisioning processes like account creation, password reset requests, account suspension and deletion and audit reporting.

Product Selection

Organizations are changing constantly, developing complex relationships with affiliates, subsidiaries, suppliers, partners and customers. Managing identities and user entitlement becomes cumbersome across such extended organizations. How can you create, modify and revoke user security profiles and rights in a centralized way, across heterogeneous IT infrastructures? Tivoli Identity/Access Manager is the answer.

IBM Tivoli Directory Server
IBM Tivoli Directory Server provides a powerful LDAP identity infrastructure that is the foundation for deploying comprehensive identity management applications and advanced software architectures.

IBM Tivoli Directory Integrator
IBM Tivoli Directory Integrator provides real-time synchronization among heterogeneous identity data sources. It allows you to establish an authoritative, up-to-date identity data infrastructure and helps maximize the return from your existing investment in directory products.

IBM Tivoli Identity Manager
IBM Tivoli Identity Manager centrally coordinates:

- creation of user accounts;
- automation of the approval process;
- provisioning of resources;
- password synchronization/resets; and
- generation of audit trails.

Tivoli Identity Manager enables you to bring users, systems and applications online quickly, thereby helps you realize operating efficiencies, reduce costs and increase return on investment.

IBM Tivoli Access Manager
IBM Tivoli Access Manager provides consistent identity-driven control from a single administration console, enabling single-policy access management across a broad range of resources. The Tivoli Access Manager family includes:

- IBM Tivoli Access Manager for e-business, which provides end-to-end security for e-business, including accommodation of multiple authentication mechanisms, Web single sign-on, URL and application-level authorization, distributed Web-based administration, and policy-driven security.
- IBM Tivoli Access Manager for Operating Systems, which protects individual application and operating-system resources by establishing rules that fine-tune access for all UNIX and Linux accounts, including super-user and root accounts.
- IBM Tivoli Access Manager for Business Integration, which enhances the native security services of
    - WebSphere MQ to provide end-to-end integrity and privacy of message data, and centralized management of both data protection and access control policy.
    - WebSphere Business Integration Message Broker and Event Broker, to provide access control for publish and subscribe rights to topics, also with centralized, policy-based management.

Vendor Selection
TCP decided to go with Trinity Solutions, a premier IBM partner because TS has a proven Security track record with sound security expertise. “The decision was simple” states Rich Davison, Security Specialist with the Children’s Place. “These guys came in and knew their stuff… and with IBM’s Identity Management products, leaders in their field, we got the best solution for the cost.”

Planning Considerations

What we thought at the time

Based on previous system deployment experience and recommendations by IBM and Trinity Solutions, the plan was to consolidate user privileges, clean them of invalid users, develop roles based on patterns of privileges, and load the db into TIM

The Children's Place would like to initially accomplish as a result of this project:

- Password and ID synchronization
- Password reset self-service
- Automatic creation of appropriate accounts
- Automatic account changes, suspensions and deletions
- Automated workflow for IT account change approval and resource procurement
- Capture and documentation of account TCP provisioning policies

Solution Architecture

Hardware

- 2.8 GHz processor
- 2 GB RAM
- Mirrored 205 GB Hard disk

TIM Server

- Microsoft Windows 2003
- DB2 8.1
- IBM Directory Server 5.2
- WebSphere 5.0.2.8
- IBM Tivoli Identity Manager 4.5.1

TIM Agent

- Tivoli Identity Manager Agent for Windows Server
- Tivoli Identity Manager Agent for Active Directory
- Tivoli Identity Manager Universal Agent for use with the Lawson HR db.
- Tivoli Identity Manager Agent for UNIX (AIX)
- Tivoli Identity Manager Agent for Lotus Notes
- Tivoli Identity Manager Agent for Tivoli Access Manager

Implementation

Connector deployment

Directory integration

Adjustments to the plan

Install Tivoli and configure all components as specified in the design and implementation plan.

Site Preparation

- Ensure systems are procured and staged in the appropriate location
- Ensure network connectivity to the systems
- Ensure account information for the systems is known
- Ensure systems are configured as expected

A site inspection with customer and contractor takes place after this activity has been completed and concludes with a sign off sheet.

Install & configure the IBM Directory Server

- Validate Microsoft Windows 2003 installation
- Install Gskit 7.0
- Install DB2 8.1
- Install IBM Directory Server 5.2
- Install IBM Directory Server client 5.2
- Install IBM Http server 1.3.28
- Install WebSphere Application Server 5.0.2.8
- Configure Directory Server on M1 as master
- Configure Directory Server on M2 as slave

Install & configure Tivoli Identity Manager Server on M1

- IBM Tivoli Identity Manager 4.5.1 server

Install and configure Tivoli Identity Manager Agents

- Install TAM Agent for ITIM
- Install Active Directory Agent for ITIM on the Windows server to synchronize users
- Install and customize Universal Agent for use with Lawson HR db

Sage Installation, Input Data Consolidation, Processing and Uploads

- Project planning
  - identify sources of data, data elements required from each, and format of consolidated user file
  - Identify repositories of defined roles and members
  - Define processes for consolidation
  - Define processes for uploads
- Task assignment to Trinity Solutions and TCP team members
- Interfaces construction and data refinement
- Role engineering
- Delivery of roles and members into repositories

- Report orphaned/abandoned accounts

Tivoli Identity Manager Customization

- Create administrative structure based on user management.
- Create TIM organizational roles for automated provisioning of the Active Directory and TAM accounts.
- Create provisioning policy by specifying role membership and service entitlements.
- Develop processes to be executed by TIM when new users are added to Active Directory manually via Active Directory native interface
- Develop processes to be executed by TIM when a request to change user access privileges is triggered by a change in the Lawson HR db.
- Develop workflow processes for approvals/denials
- Create a password policy for the three relevant resources
- Add additional attributes for TAM role
- Setup automated reconciliations with TAM, Active Directory and Lawson HR db

Implementation Review:

- Create and submit Deployment Document for approval.
- Demonstrate functionality
- Incorporate recommendations and submit the final document for review.

Project results

What we learned about planning and implementing IAM
ITIM is a solution composed of various infrastructure pieces such as: WebSphere Application Server, HTTP Server, RDBMS, LDAP Directory, MQ series (it is also used under the covers for the workflow). We installed all the pieces on a single server which made it relatively simpler to manage.

At TCP we decided to install with WAS, and DB2. They are included free of charge in the ITIM package, to be used solely for ITIM, you can install these components on the ITIM server (Single Server Installation) or on separate machines (Cluster Installation) and you don't have to worry about licensing issues, they are included in the base ITIM license.

Installing the ITIM server seemed simple and straight forward, configuring of the agents required some attention to the SSL communications, which require a Digital Cert to function properly. All communication between the ITIM server and each agent component is done over an SSL connection.

Configuration of the ITIM server requires a lot of careful planning. An organization structure is required to place all of the Identities that you are going to manage, we used our HR structure. The organization structure also can segregate your Admin Domains (East Coast versus West Coast) as well as Services (Active Directory, LDAP, Lotus Notes) you are going to be provisioning. Our model was simple as we placed all of our Services at the corporate level so they were available

across our entire Organization. We chose not to define any Admin Domains as all of our administration is going to take place in one location. ITIM is very driven to Role Based provisioning, which requires you to create roles like: User, SysAdmin, Operator, etc. Once created and an organizational structure is implemented, then you assign persons to those roles in order to provision IDs on your servers. This part of the implementation can be lengthy as it requires time to make a detailed study of existing accounts that have to be mapped in the new roles. Caveats such as linking usernames across heterogeneous accounts can be challenging. Linking users to aliases like Name changes, misspellings and nicknames proved to be an arduous task as well

Once we had our organization loaded, we used a DSML Identity feed to load in our employees (Person Records). The employees are dynamically placed into their correct Department using a placement rule and Accounts are automatically suspended or restored based on their status in HR. This feed also creates all the necessary aliases that a Person may require. For example you may need to limit user ids to eight characters for certain platforms (AIX), a second alias may be to limit the user id to twelve characters (AS/400), and a third may be the person's full name.

Services are then defined to connect to each Agent you have installed. After you define a Service you must create a Provisioning Policy for the service (or Service Profile) that says who may have an account on the Service. You can restrict a service to only be available to a Person and not to a Business Partner Person as an example. Now that your service is defined and a Provisioning Policy is in place you can bring in all of your existing accounts by running (or scheduling) a reconciliation. The process is very straight forward as the accounts are brought into ITIM they are associated with an identity based on the aliases you defined earlier. Any account that is not matched becomes an Orphaned account and can be easily identified by running a Reconciliation Report.

Caveats such as linking usernames across heterogeneous accounts can be challenging. Linking users to aliases like Name changes, misspellings and nicknames could prove to be an arduous task as well.

The most time consuming issues in ITIM was the Role Engineering required to establish the base of the Provisioning Policies that make ITIM work. ITIM is very driven to Role Based provisioning, which requires you to create roles like: User, SysAdmin, Operator, etc. Once created and an organizational structure is implemented, then you assign persons to those roles in order to provision IDs on your servers. This part of the implementation can be lengthy as it requires time to make a detailed study of existing accounts that have to be mapped in the new roles.