Banner, BEIS and Active Directory
Identity Integration

Presented by: Khouloud H. Hawasli
St. Louis Community College
March 21, 2011
Session ID 4059
Introduction

• Review how St. Louis Community College (STLCC) integrated SunGard Banner 8.3 as the authoritative Enterprise Resource Planning system with the College's Active Directory 2003 (AD) authentication system by architecting an integrated solution that promoted consistent provisioning and de-provisioning policies and unified account management processes.

• This session is for Banner institutions who are interested in identity integration with Microsoft Active Directory to hear about the path STLCC took and the lessons learned from STLCC implementation from beginning to end.
About the College

• Largest community college system in Missouri
• District encompasses 718 square miles
• Four campuses
• Three education centers
• Numerous satellite locations in area business, industrial, neighborhood and educational sites
• 29,128 students enrolled in credit courses (Fall 2010)
• 3,823 full- and part-time employees
Agenda

STLCC Environment

Planning and Setup

Identity Integration Framework

Architecture Design

Outcomes
STLCC Environment
STLCC Infrastructure

- SunGard Higher Education Banner ERP system
- Single forest, single domain Active Directory (AD)
- All administrative, and most student/library workstations are running Windows XP – 5,000+ desktops
- All employees log in through AD accounts
- All employees have on premise Exchange mailboxes (@stlcc.edu)
- All students have a Microsoft hosted Windows Live e-mail account (@my.stlcc.edu)
- Growing use of Blackboard LMS (Enterprise 8)
- Do not have Luminis Platform
STLCC Infrastructure

- Banner is the trusted source for all human resources and student information

- Already have district-wide AD authentication in place, Domain Controllers were sized for multiple years of student accounts

- Account ID created by Banner (3rd Party ID)
  - Became the AD sAMAccountName
  - Became the Windows Live account prefix
Data Processing

- CSV files were generated overnight for new employees and students

- Employees’ accounts and mailboxes were provisioned using VBScript

- Microsoft Identity Integration Server (MIIS 2003) was provisioning
  - Students AD accounts when they register, but are disabled
  - Student e-mail accounts (Windows Live@edu)
Institutional Challenges

- Users are confronted with an overwhelming number of different usernames and passwords
- Increased risk of inappropriate access
- Increased productivity loss
- Increased demand for agility
IT Challenges

- Duplicated efforts are everywhere
- Identities, credentials are provisioned across multiple applications
- Identity management became:
  - High cost
  - Difficult for custom-coded solution
- Increased helpdesk calls for locked accounts
- Limited IT server support staffing
- Limited help desk support staffing
Objectives

Strategic

• Design an identity integration system to facilitate the implementation of common credential to ease the management and access to college resources

Tactical

• Provide access to appropriate applications and systems near real-time
• Align provisioning and access with business policies
• Simplify and secure access to college resources
• Improve customer experience
• Reduce IT cost for identity management
• Implement a common-credential
Technical Objectives

- Designate Banner to serve as the authoritative role for authorization using role based access control

- Implement Banner Enterprise Identity Services (BEIS) to transit role and identity information driven by triggered events in real time for consumption by Microsoft Identity Lifecycle Manager 2007 (ILM)

- Designate Microsoft Active Directory (AD) as the main college authentication system
Planning and Setup
Planning and Setup

Setup an R&D environment

Setup discovery workshop

Define the best path for the integration for the environment

Develop an integrated structure to promote the consistent interpretation and enforcement of policies
Planning and Setup

Review the current processes
- Employees
- Students
- Others

Identify the data elements in Banner that are necessary for identity integration
  Simplify the data element mapping

Design Active Directory OU structure
  Keep it simple
Planning and Setup

Banner Preparation

- Banner General 8.2, plus patch 8.2.0.1
- Banner Intcomp 7.3.0.2
- Oracle Database 10gR2 or higher
- Oracle Application Server 10gR2

Granted appropriate access to new tables and processes

Configure GUASADM

Configure GTVSDAX
Identity Integration Framework
Integration Components

- **Banner Enterprise Identity Services**
  - Customized LDAP web services
- **Microsoft Lightweight Directory Services**
- **Microsoft Identity Lifecycle Manager**
Identity Integration Framework

New Students
New Employees

Roles:
Basic
Employee
Student
AppAccept

Microsoft Active Directory
Microsoft Identity Lifecycle Manager

Banner General Person Repository

EMPLOYEE Module

STUDENT Module Tables

Role Calculation

GORRIROL Roles Tables

Banner Enterprise Identity Services Middleware

Integrated Directory

Microsoft LDS

Identity XML

SPML
Banner Enterprise Identity Services

GORRSQL
• Business rules form used to define additional data elements

Extension Elements
• Data elements added to the base set of information published

Roles
• Assigned based on existence of data in specific tables
• Stored in GORIROL table and initially populated by GURIROL process
• Role Changes to GORIROL produces SPML messages
Banner Enterprise Identity Services

Gateway – part of BEIS middleware
• Generates GUID
• Transforms XML message into UDCIdentity Message
• Publishes UDCIdentity message to SPML topic for consumption

Proxy – central component of BEIS
• Conduit between SunGard applications and central identity vault using SPML
Customized SunGard LDAP Web Services

A Services Oriented Architecture (SOA) written to handshake with the central system, the Microsoft Lightweight Directory Services (LDS), via Web Services Description Language (WSDL) and Simple Object Access Protocol (SOAP)

— Used to interconnect the two core infrastructure systems
— A connector to communicate to the LDS instance and populate identity information in real time using Oracle stream technology
— Feeds the selected directory Information to LDS from the Banner tables
Banner LDAP Web Services

Create User

Banner Identity Gateway → Oracle → Enterprise Identity Proxy Services

Banner Identity XML

Application Server

Oracle

SPML 2.0
UDC
Identity XML

Provisioning

Microsoft AD LDS/ILM

Provision User

Microsoft Active Directory

Rules

GTVSDAX Rules

Capture and Apply Process [Oracle Streams]

GORRSQl Rules

PSP Connector

Handshake via WSDL and SOAP
Dataflow in Banner Enterprise Identity Services

Demonstrate Dataflow When Banner Event Occurs

Session ID 4059
Lightweight Directory Services

An independent mode of Active Directory that provides dedicated directory services for applications

LDAP-compliant directory service

Operates independent of Active Directory and supports the use of LDAP over SSL and facilitates synchronization of information with AD DS

Provides a view for users information and identity attributes
Lightweight Directory Services

Simple directory structure for future expansion

Select attributes matching to Active Directory to simplify provisioning and future development

Can be replicated for redundancy and high availability

Secure access to the directory

Select multi-value attribute for roles
Sample of Mapping Data Elements

(*) Extension Elements

<table>
<thead>
<tr>
<th>Banner</th>
<th>LDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDCIdentifier</td>
<td>cn</td>
</tr>
<tr>
<td>*PIDM</td>
<td>employeeNumber</td>
</tr>
<tr>
<td>*ID</td>
<td>employeeID</td>
</tr>
<tr>
<td>GivenName</td>
<td>givenName</td>
</tr>
<tr>
<td>MiddleName</td>
<td>middleName</td>
</tr>
<tr>
<td>FamilyName</td>
<td>sn</td>
</tr>
<tr>
<td>*EmailAddress</td>
<td>mail</td>
</tr>
<tr>
<td>*ALIAS</td>
<td>samAccountName</td>
</tr>
<tr>
<td>*CampusPhone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>*TITLE</td>
<td>title</td>
</tr>
<tr>
<td>*Location</td>
<td>company</td>
</tr>
<tr>
<td>Institution roles</td>
<td>carLicense</td>
</tr>
</tbody>
</table>

Session ID 4059
Microsoft Identity Lifecycle Manager

- Provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials
- Provides identity synchronization and user provisioning in a single solution
- Ensures access to college resources is revoked automatically for employees who leave the organization
- Defines and automates the processes used to manage identities from creation to retirement
- Automatically creates user accounts, mailboxes, home folder, map drives and other identity information in Active Directory in near real-time
Microsoft Identity Lifecycle Manager

- **Synchronize Identity Information**

- **Manages identity information by aggregating it in a central repository called the metaverse.**

- **Management agents serve as connectors that translate data from these connected stores to the metaverse.**
Identity Lifecycle Manager Provisioning Steps

1. A new user is triggered into LDS
2. LDS-MA runs in import mode and creates a new object LDS connector space.

3. LDS MA runs in synchronization mode and projects new connectors into the Metaverse, a new Metaverse object is created that corresponds to the new connector. As ILM is configured for provisioning, the provisioning code runs and a new pending export is created in the AD-MA connector space.

4. A new Active Directory user account is created the next time the AD-MA runs in Export mode.

5. During the next import run – which may or may not be immediately – the new object will be confirmed (and any required AD-generated attributes will be imported – maybe an email address).
Demonstrate Dataflow When ILM Synchronization Occurs

AD Lightweight Directory Services
Data Elements updated by GORRSQL rules integrated with Banner.
The consumer of SPML 2.0 UDC Identity XML.

Synchronization process creates an integrated view of the data stored in the connected data sources.

1. Change occurs in a LDS table

2. LDS Connector Space
3. Metaverse
4. AD Connector Space
5. Export

Session ID 4059
Architecture Design
Middleware Architecture Overview

Banner Enterprise Identity Services:
Extension elements and roles are configured in GORRSQL and change capture rules are configured in GUASADM.

Microsoft Identity Lifecycle Manager:
Identity Management rules are configured in the management agents.
Identity Lifecycle Manager Design Overview

Standby for emergency only

Session ID 4059
Results

A person gets entered in Banner
• Creates the person record with a unique PIDM
• Triggers the unique UDCIdentifier

A SOA protocol
• Feeds the selected directory Information to LDS from Banner tables

ILM management agents
• Keeps information in both LDS and AD in sync
Results

In near real-time, automatically provisioning, de-provisioning and managing

- Faculty and staff accounts, Exchange mailboxes, home folder and mapping home drive
- Students’ account and Windows Live@edu email accounts

Updating directory information near real-time

- Title, department, campus, phone numbers… etc.

Improved our SLA for accounts provisioning from 24-72 hours to 1 hour
Lessons Learned

• Communicate with all stakeholders throughout the project and have a clear understanding of your organization expectations (real-time vs. near real-time provisioning)
• Prioritize desired functionality
• Don’t implement BEIS until you are on Banner 8.3
• Plan thorough well-timed training
• Document each part of the process so it can be repeated
• Rollout each middleware in stages
• Create a server batch job to clear the locked file when server reboots unexpectedly so BEIS will connect to the database correctly
• Develop a recovery process for loss of data
Summary

• Outline your processes before you start and organize your project carefully

• Banner Enterprise Identity Services can help automate provisioning processes in real time

• Banner triggers and roles can streamline processes

• Microsoft Identity Lifecycle Manager can make the automation complete and help manage identity lifecycle
Questions & Answers
Thank You!

Khouloud H. Hawasli
Manager, Electronic Communications and System Integration
khawasli@stlcc.edu
(314) 539-5090

Panelists:

Joy Hayward
HR/Payroll System Leader
jhayward2@stlcc.edu

Joan McCready
Student System Leader
jmccready@stlcc.edu

Please complete the online Session evaluation form

Session ID 4059