HARVARD UNIVERSITY
Information Technology

Identity and Access Management
PI-1 Demo

December 2, 2014	Tuesday	10:00 A.M.	6 Story Street

Agenda

- Meeting Purpose and Intended Outcomes (5 min)
- PI-1 Business Objectives (5 min)
- Demo: User Data From the Source to SailPoint (5 min)
- Demo: Claiming a New User Account (10 min)
- Demo: Import Alumni Using New Identity API (5 min)
- Demo: Migrating HMS Users to 0365 Using FIM (5 min)
- Update: Cloud Migration Progress (5 min)
- Summary and Close

Meeting Purpose and Intended Outcomes

Purpose

To provide the team and invited guests with a summary and demonstration of key work that has been accomplished during Program Increment 1 (PI-1).

Intended Outcomes

- Share our work in PI-1 and allow stakeholders to provide feedback
- Continue to build understanding of the IAM program

PI-1 Business Objectives

Teams accomplished the following objectives:

Objective	Demonstration
Implement data model to support migration of HMS and Alumni	• Migrate Alumni data into IdDB
Develop data migration methods	• Provision 0365 for HMS • Import alumni data via Identity API
Prepare to enable development of claiming and provisioning during the next program increment	• SailPoint aggregating user data from multiple sources • Self-service process for claiming a new account that integrates with Sailpoint/IIQ
Network design to support cloud migration	• Presentation on LDAP

Demo: User Data from the Source to SailPoint

- Data is generated by source systems of record and fed to the central IdDB identity database, which is an **identity registry**.

- **IdDB has a master data record** of each Harvard user, and SailPoint uses this to drive the provisioning system

- SailPoint IdentityIQ **"identity cubes"** aggregate data from the IdDB source and then provision out to target systems

Ken Schwartz will demonstrate source data from IdDB and relate it to the identity cubes in SailPoint/IIQ.

Recap: User Data from the Source to SailPoint

We saw:

- Source data in IdDB (via MIDAS) that is the basis for provisioning
- Source data aggregated in SailPoint/IIQ cube
- Details of not only source data, but also provisioned data aggregated for a user in IIQ

Benefits:

- Enable provisioning of Alumni users for authentication and access to resources

Demo: Claiming a New User Account

- User data is aggregated in the provisioning system, but in order for a user to access resources, he or she **needs to claim an account**

- Business units (Student Admissions, Human Resources, Academic Affairs) facilitate the myriad processes that onboard a new user; they will **continue to control** when a user is invited to claim a new account

- Our demo shows a **new employee claiming an account** after receiving an email containing their new HUID

Vanja Kojuharova will demonstrate self-service account claiming (creation).

Recap: Claiming a New User Account

We saw:

A prototype of a new self-service process allowing new employees, students, or POIs to create a new Harvard account integrated with SailPoint/IIQ — **this is a foundational business process for account management**

Benefits:

- Self-service user onboarding for account creation that can be deployed flexibly by schools and departments
- Unified process for employees, students, and POIs that will be consistent across Harvard, resulting in less user confusion and improved Service Desk support

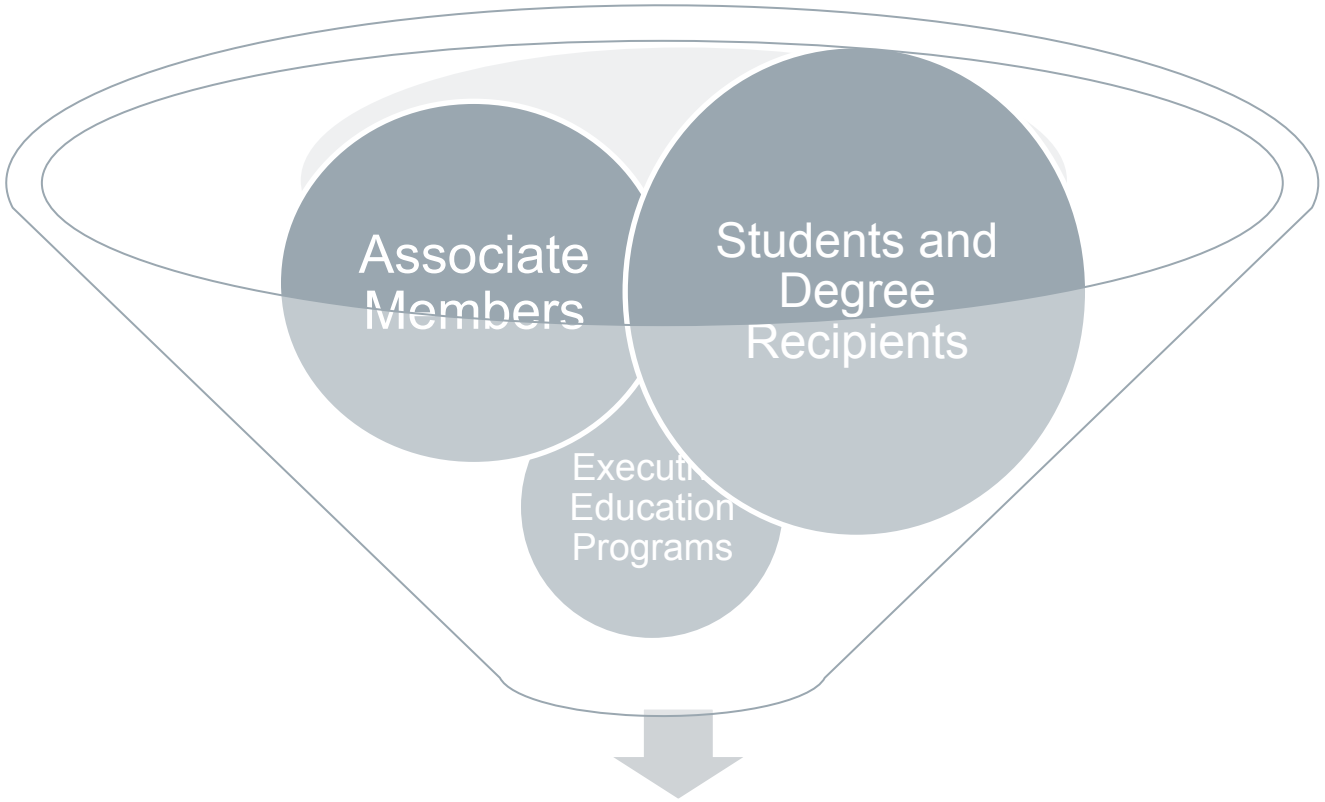
Demo: Import Alumni Using New Identity API

- **Our top goal for FY15:** Replace the Alumni user management and authentication systems

- **The first step:** Incorporate Alumni data into the identity registry to enable HUIT to provide account management services and user provisioning — allowing Alumni users to authenticate using a Harvard-issued credential

- Our demo will go by in the blink of an eye — but it uses a **new data model** that incorporates alumni roles into IdDB, and a **new RESTful API** to enable the Alumni team to feed their data to support account management and provisioning

Background: Various Alumni Populations Make Up Our User Base



More Than 380,000 Alumni

Our Challenge: Improve Process and User Satisfaction

Improve End User Experience

- Eliminate the need to register with HAA – we already know you!
- Allow student accounts to keep working forever
- Use standard processes for account management
- Enable coordination of service desks and customer service

Expand Access to Resources

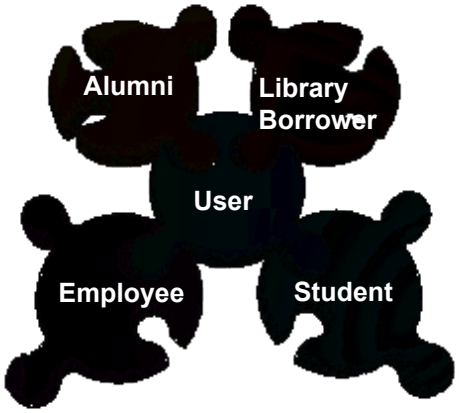
- Make it simpler for application owners to extend access Alumni
- Provide clearer information on what resources are available
- Position us to offer services to additional stakeholders in future – donors, parents, friends

Balance Convenience & Security

- Improve self-service password reset by capturing password recovery information provided for account management
- Strengthen the passwords and the process
- Tailor onboarding processes to meet HAA needs

Step One: Import Alumni Data Into IAM

Explained: Alumni Data in IAM



Alumni Role(s)

- Start Date
- End Date
- Role Type
- School Affiliation
- Degree
- Year

Each **Alumni Role** has an associated **Role Type** that explains their Alumni affiliation:

Program Participant, Alumni, Student, or Associate Member

Addresses

- Address information
- Alumni-specific address types: business, home, seasonal

Alumni may have multiple **Email Addresses** on file:

Preferred Email is the most important one for Alumni

Demo: Import Alumni Using New Identity API

Enable Alumni Group to add four new types of people with Alumni roles:

- Alumni
- Current students (future graduates)
- Associate members (non-traditional students)
- Program participants

Amy Fairhall will demonstrate:

1. Raw data containing information on Alumni role to be added to an individual (in proper format to be submitted to the new API)
2. Submission of data to the API
3. Viewing the additional role added to the individual

Recap: Import Alumni Using New Identity API

We saw:

Use of the new Identity API to import alumni data into IdDB — a foundation that will enable us to provide Alumni account management and provisioning (FY15 IAM Goal)

Benefits for the Alumni user:

- User's identity remains constant throughout the lifecycle of Harvard affiliation
- Improved self-service experience for password reset and account management
- As students graduate and transition to Alumni status, no additional registration will be required in the future
  - However, transition *will* require existing Alumni users to re-register
- Access to resources is granted or removed automatically
- Expanded common person data model provides new options for internal service providers to offer Alumni access to resources
- Enables integration with ID card privileges and related physical access

Demo: Migrating HMS Users to O365 Using FIM

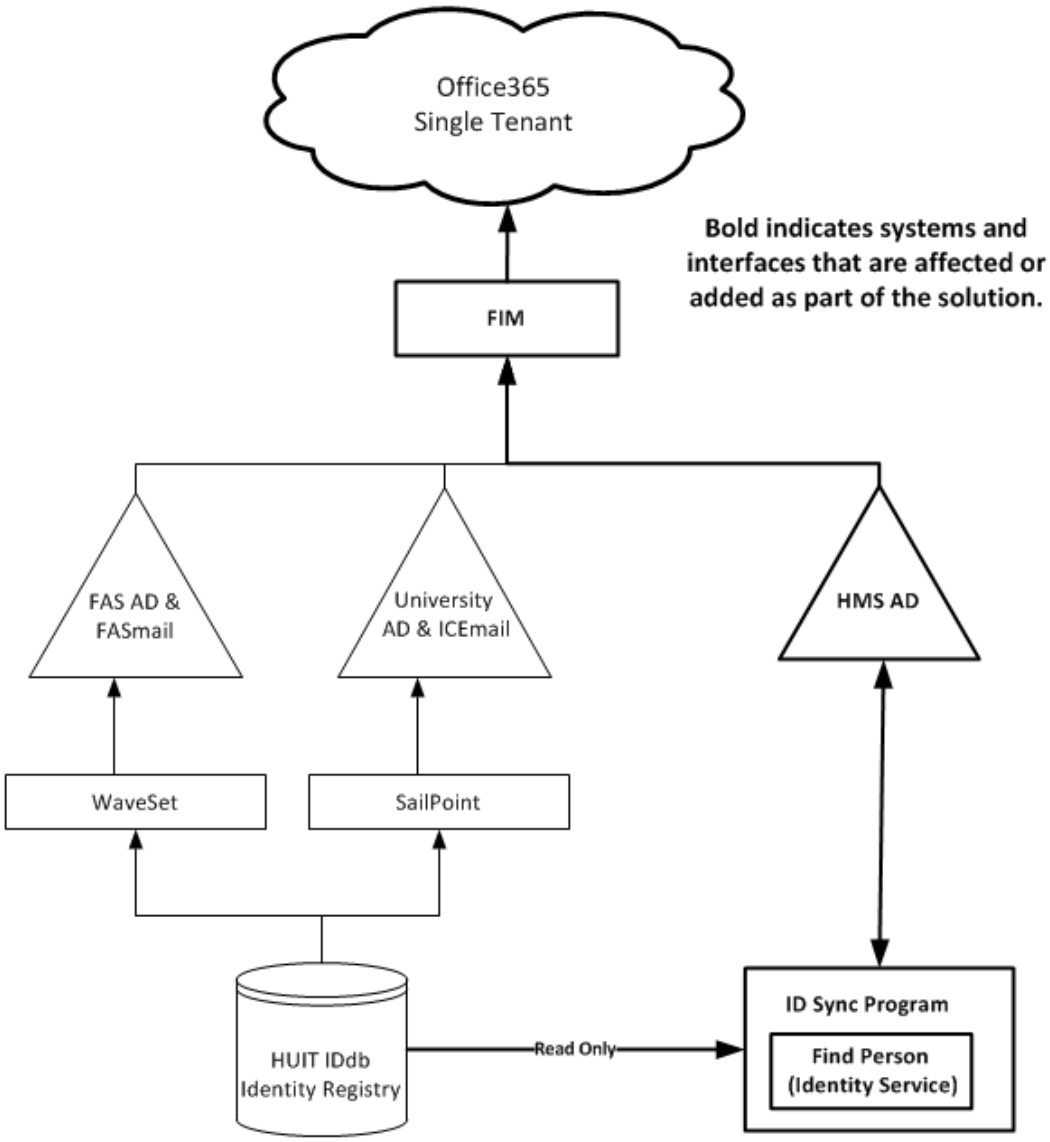
- We are supporting provisioning HMS users to O365 by syncing identity data from the identity registry (IdDB) — as well as the HMS Active Directory — to 0365 using Microsoft's FIM provisioning tool

- This enables the Medical School to migrate users to O365

- Our bridging strategy leverages current HMS users in our identity registry and universal unique identifier (UUID) to consolidate HMS users in the single O365 tenant, enabling easier collaboration

Terry Connolly will demonstrate what data looks like before (HMS AD) and after in the O365 Azure AD.

HMS to O365: Bridge Solution Architecture



HMS to O365: Bridge Solution Goals

The bridge provisioning solution met the following goals:

- Decommissioned HMS O365 tenant and moved to HUIT O365 single-tenant platform
- System provisions users in HMS AD to O365 Azure AD through FIM (MS Identify Management System), consistent with other HUIT-managed ADs
- Solution in place and ready for HMS to migrate users off outdated Exchange server

HMS to O365: Development Highlights

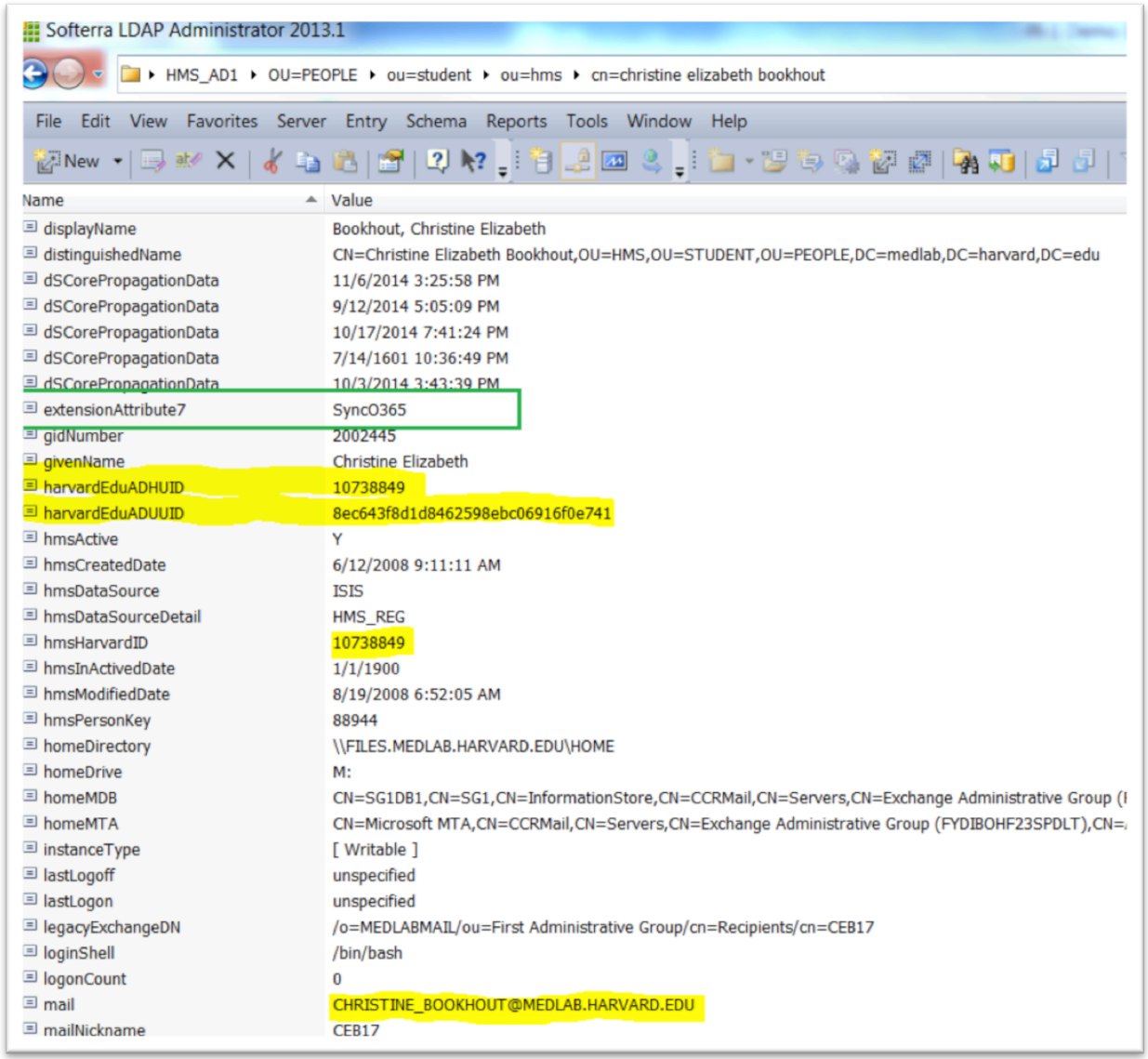
FIM (MS Identity Management System):

- Updated to include HMS AD connector and provisioning rules
- “Pending Exports” report for analysis prior to committing changes
- IAM assumed responsibility for Harvard FIM instance

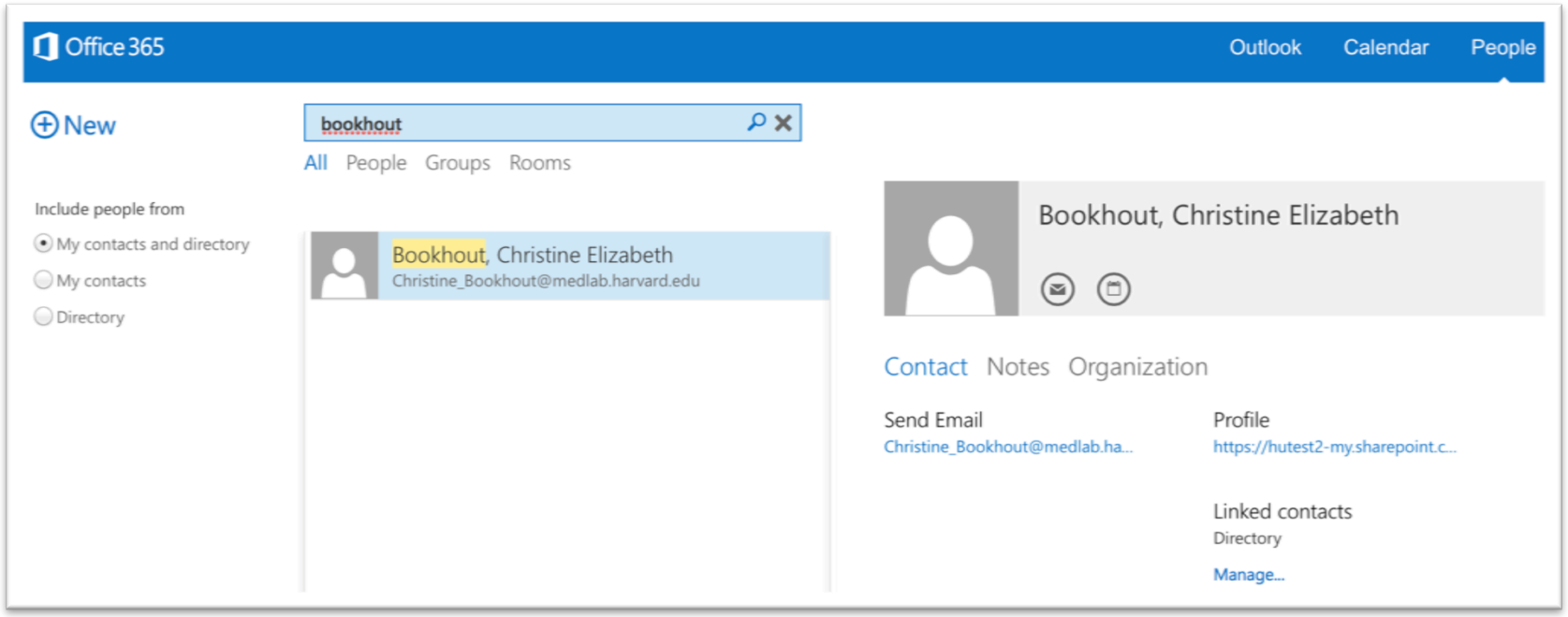
IdDB Sync:

- Cloud-based web service developed by IAM
- Adds UUIDs to HMS AD for identity mapping and provisioning
- Uses new Identity Services (FindPerson)
- Test mode capability, audit logging, and exception reporting

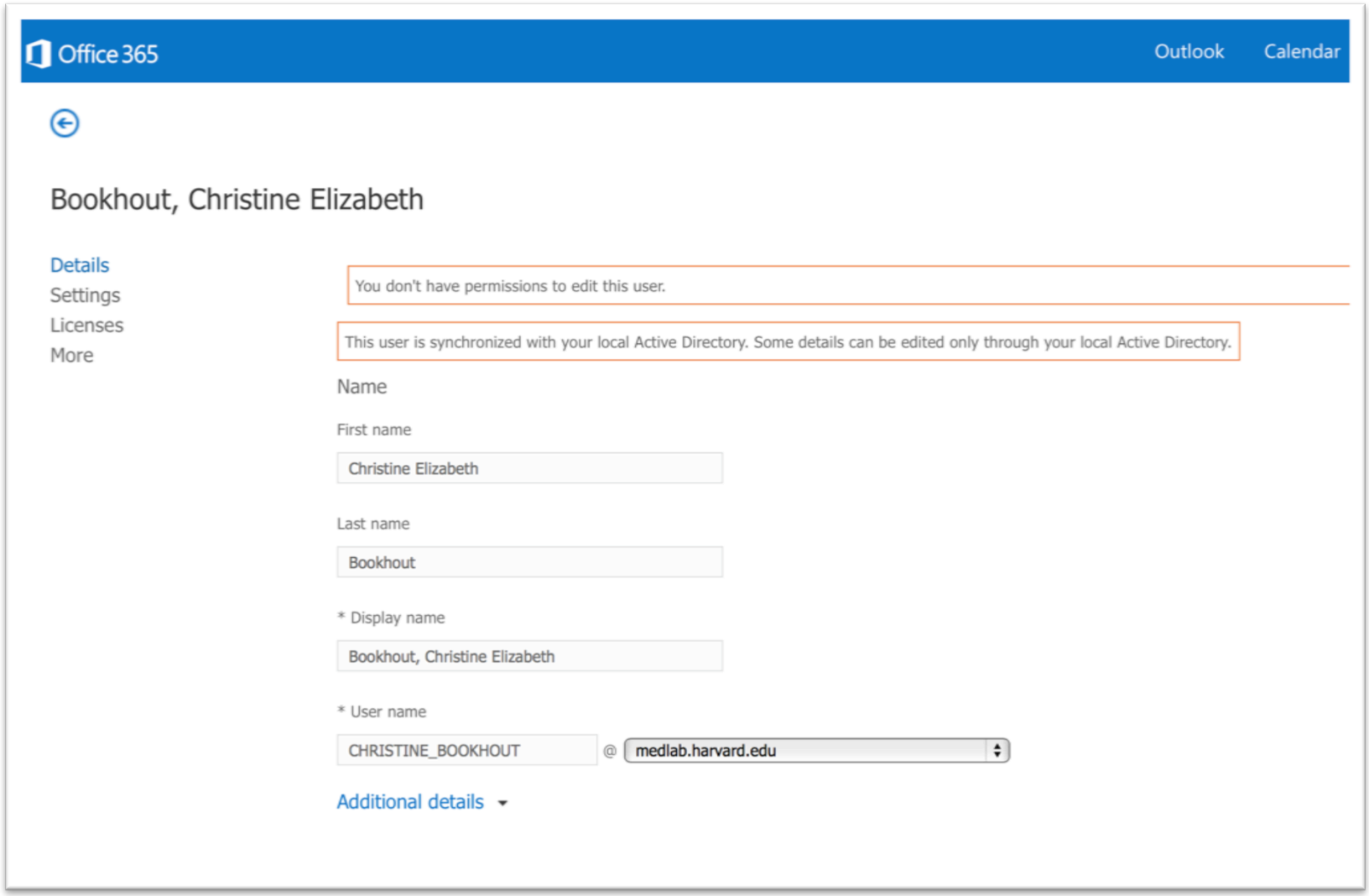
HMS to O365: User Entry in HMS AD After IdDB Sync is Run



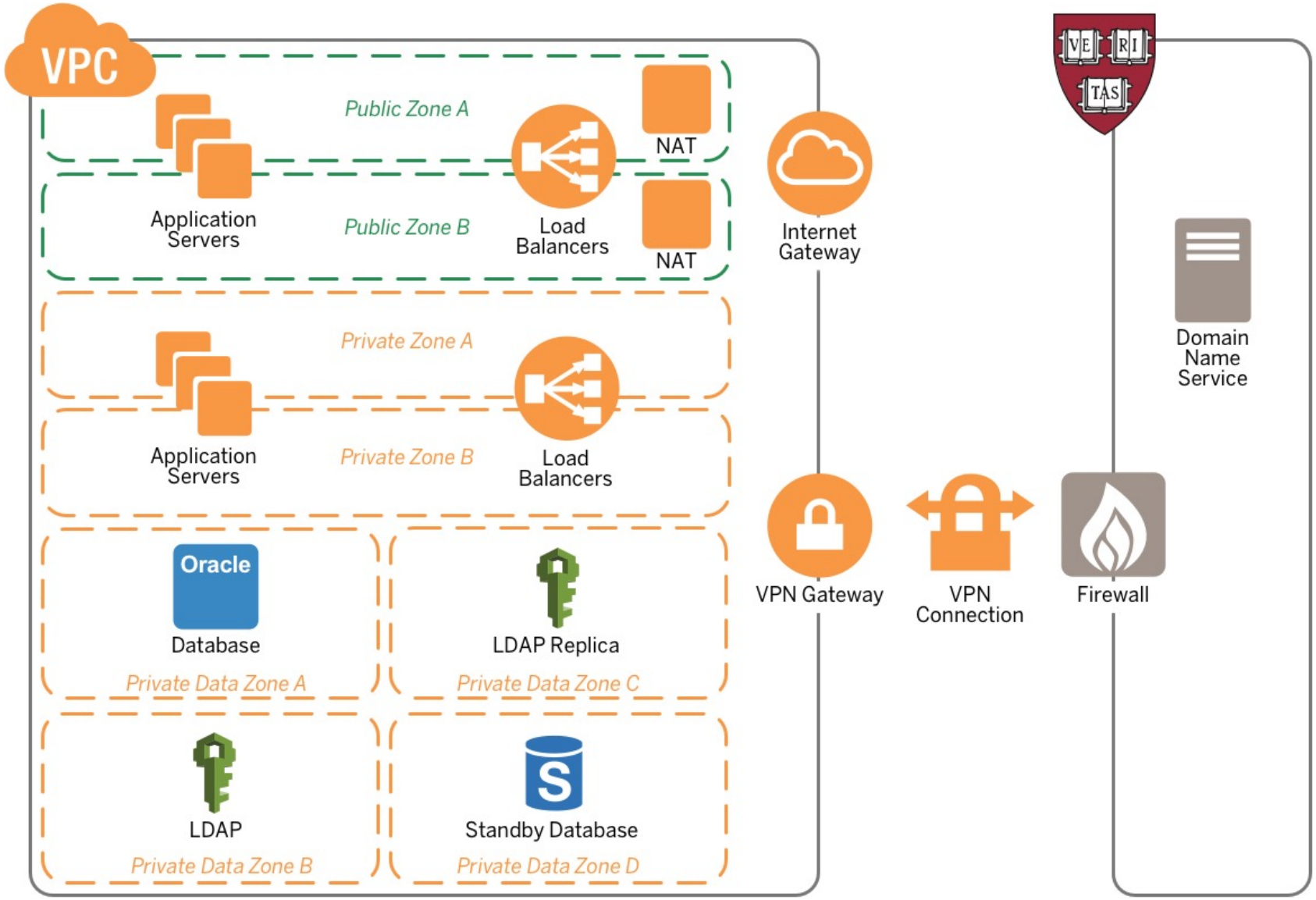
HMS to O365: User Entry in Azure AD After FIM is Run



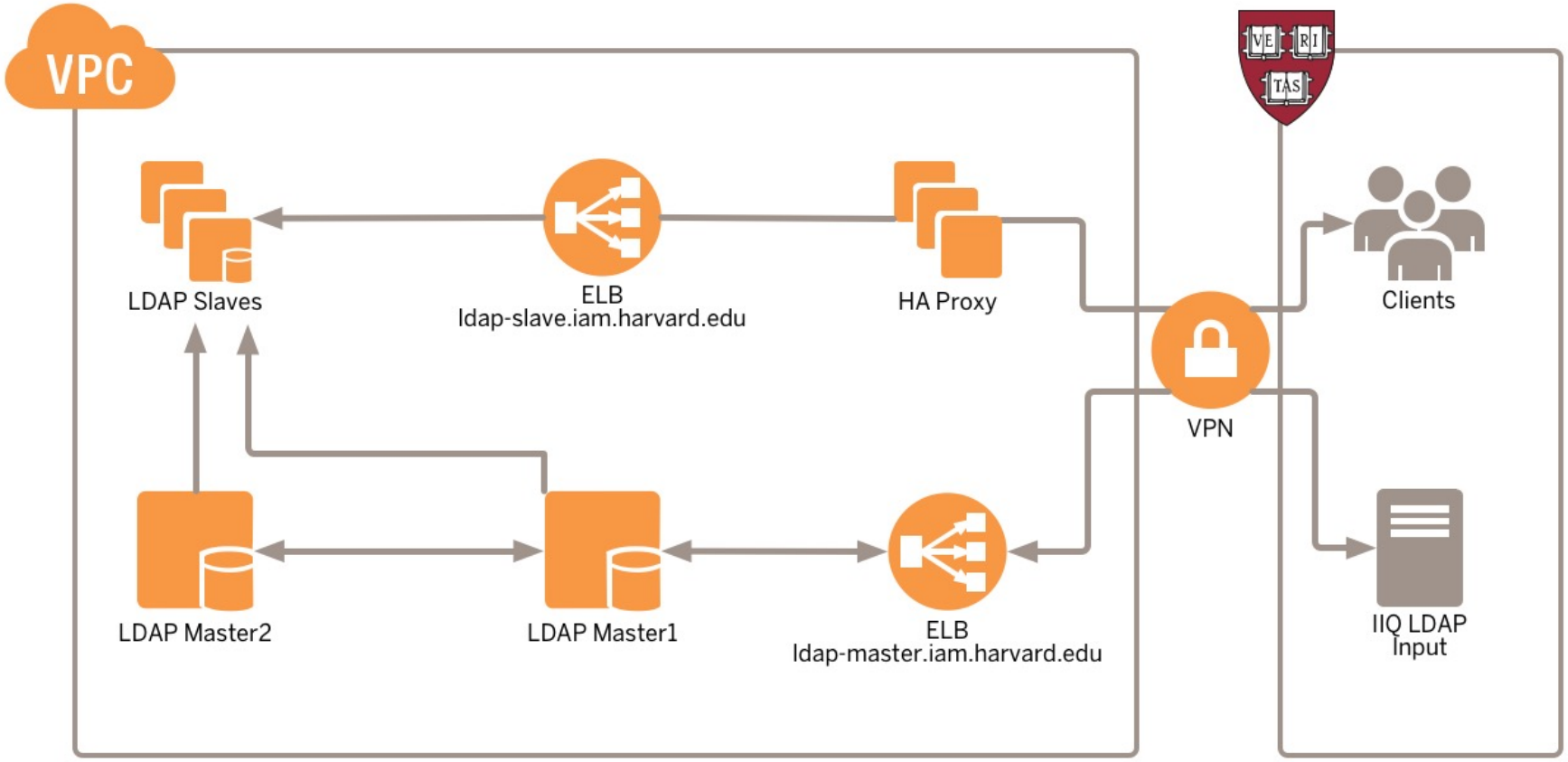
HMS to O365: User Entry in O365 Admin Console After FIM is Run



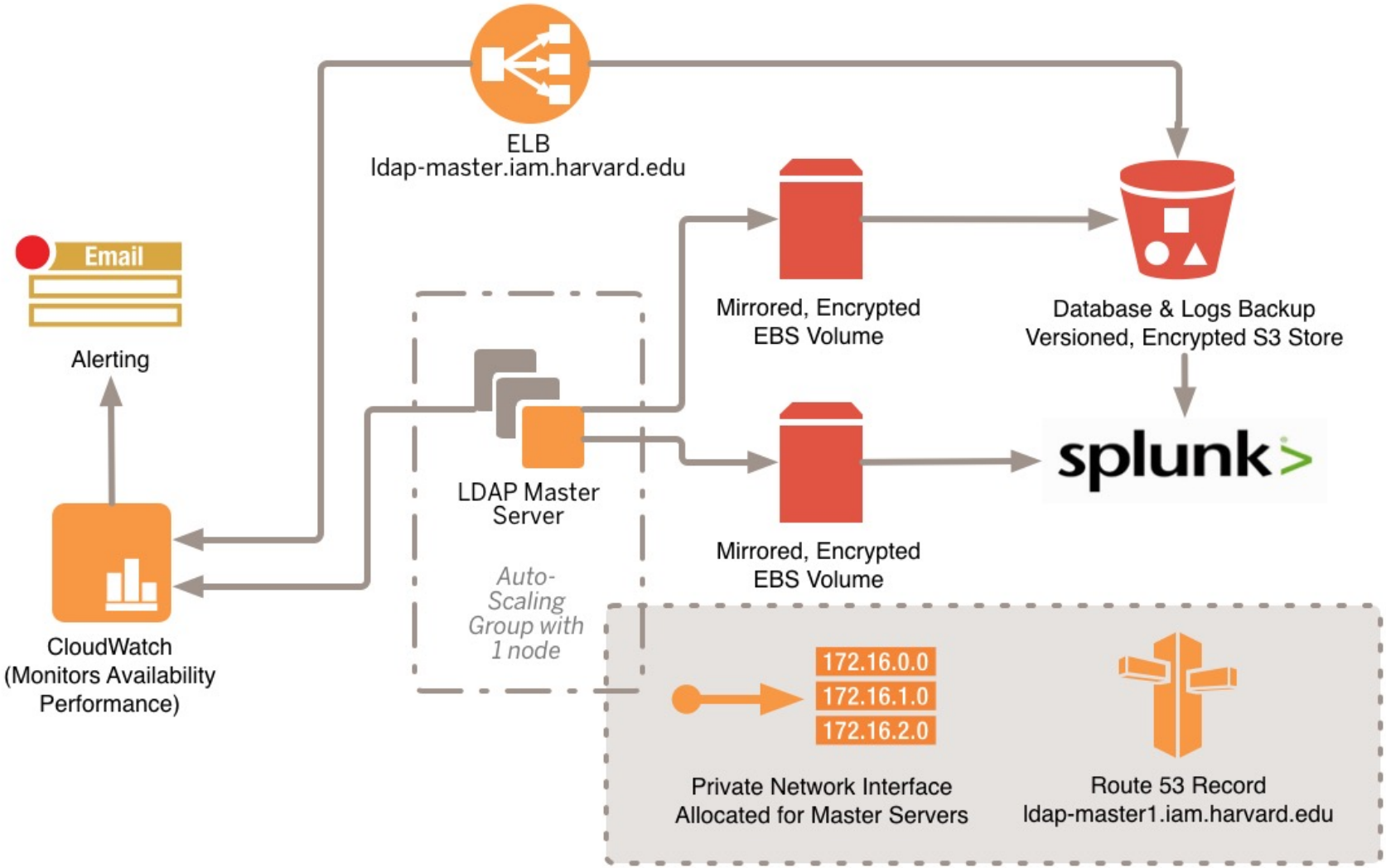
Cloud Migration: Network Extension of Harvard Data Center to AWS



Cloud Migration: Harvard LDAP on AWS



Cloud Migration: Overall Progress



Summary: Status of PI-1 Business Objectives

The team met the following objectives:

- Deployed new data model for Alumni data
- Completed API for Alumni data migration
- Deployed a solution for HMS to use for migrating users off outdated Exchange server
- Prepared for development of claiming and provisioning in next program increment by building an account claiming application integrated with SailPoint/IIQ
- Deployed cloud-based environment for new LDAP (needed for Alumni data)

Summary: Status of PI-1 Business Objectives

Priority lowered due to resource constraints at HMS:

- New data model for HMS non-employee, non-student populations

Summary: Other Accomplishments During PI-1

- Deployed FindPerson API **for SIS Wave 0**
- Deployed new Connections API and ‘Facebook Printing’ capability **for HLS**
- Deployed new PeopleSoft Import so that directories and authorization services can be enhanced in the future **for all Schools per Provost’s request**
  - ORCID Open Researcher and Contributor ID
  - Academic Primary job indicator
  - Department Official Name

Questions or Feedback?

Thank you!

HARVARD UNIVERSITY
Information Technology