



Under the Hood of Fermilab's Identity Management Service

Al Lilianstrom and Dr. Olga Terlyga

NLIT 2016

May 4th, 2016

About Fermilab

Fermilab is America's particle physics and accelerator laboratory.

- Our vision is to solve the mysteries of matter, energy, space and time for the benefit of all. We strive to:
- lead the world in neutrino science with particle accelerators
- lead the nation in the development of particle colliders and their use for scientific discovery
- advance particle physics through measurements of the cosmos

Our mission is to drive discovery by:

- building and operating world-leading accelerator and detector facilities
- performing pioneering research with national and global partners
- developing new technologies for science that support U.S. industrial competitiveness

www.fnal.gov

Under the Hood of Fermilab's Identity Management Service

Fermilab is working on the implementation of a digital identity management (IdM) solution. This technical talk will discuss how we are implementing the solution - from proof of concept to go live.

This talk will cover:

- Application implementation
- Integration with downstream cloud and on-premise services
- Integration with applications that are not supported by the IdM software
- Integration with our cloud based human resources system
- Building environments for development, quality assurance, and production
 - working across multiple service owners and efficiently utilizing the resources available at Fermilab
- Preparing production services for integration with the identity management service

Timeline

- 2011
 - Ongoing IdM project canceled
 - Vendor A IdM proof of concept (POC) installation at Fermilab
- 2013
 - Dell successfully completed a POC installation at Fermilab targeting our Active Directory and Kerberos environments
- 2014
 - Decision made to implement D1 IdM
- 2015
 - Start of project
- 2016
 - Go Live

Project Scope

- D1 IdM feature set is extensive
 - Phased implementation
- Phase 1
 - Replace our existing custom account provisioning system
 - Manual interaction required by Service Desk staff
 - Automation based on Human Resources data
 - Username generation and account provisioning
 - Attribute updates
- Phase 2
 - Implement roles for provisioning access to resources
- Phase 3
 - Extend D1 IdM to additional service providers

Implementation

- Fermilab Phase 1
 - Three stages
- Stage 1
 - Connect to our Central Authentication Services
 - Two Active Directory domains
 - One Kerberos realm
- Stage 2
 - Connect to HR system
 - PeopleSoft at project start, now WorkDay
- Stage 3
 - Go Live replacing custom account provisioning system

Implementation

- Stage 1 – Connect to Active Directory and Kerberos
 - Kerberos – Unsupported by D1 IdM
- Stage 2 – Integrate with HR
 - After the D1 IdM POC Fermi replaced PeopleSoft with WorkDay
 - WorkDay supports SCIM for integration
 - The version of D1 IdM being implemented does not
 - Fermi staff created custom WorkDay integration to communicate with IdM
 - Dell wrote web service to accept data from WorkDay
 - Basic end to end plumbing test was successful
 - Accounts created and managed based on information provided from WorkDay

Implementation

- Stage 3 – Go Live
 - Special account integration
 - Service Desk interface
 - Acceptance testing  Current State
 - End to end
 - Based on HR service use cases
 - Real work
 - Onboarding, off-boarding, changes, updates
 - Not just hire and terminate
 - Change from employee to user to contractor
 - Move to QA
 - Repeat testing
 - Move to Production

Integration with Supported Applications

- Fermi uses Active Directory (AD) for our production desktop environment and for a LDAP authentication service
 - Users, employees, and contractors (as necessary) get accounts in both Active Directories as part of the provisioning process
- D1 IdM directly supports integration with AD
 - Configuration item
 - Requires a Service Account in the destination AD
 - This account needs the appropriate access to your AD
 - Default is Domain Administrator...

Integration with Unsupported Applications

- D1 IdM does **not** support integration with a Kerberos realm
- Fermi uses a Kerberos realm to provide central authentication for our Linux systems
 - As with AD users, employees, and contractors (as necessary) get an account in the Kerberos realm as part of the provisioning process
- POC used plink (open source SSH client) to issue commands from IdM to Kerberos realm
 - Less than reliable...

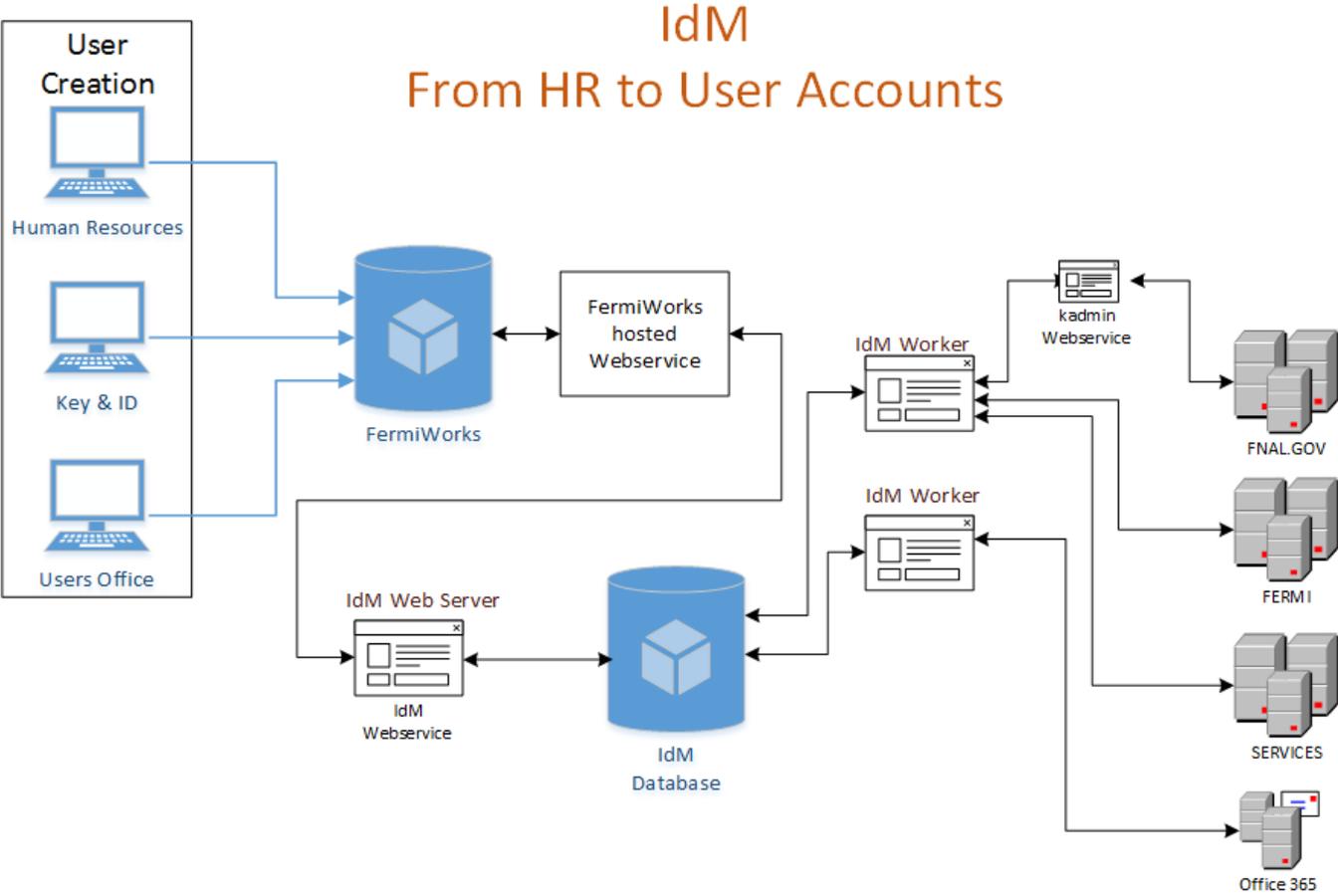
Integration with Unsupported Applications

- Fermi staff created a web service for D1 IdM to use to manage the Kerberos environment
 - Virtual machine in our central virtual infrastructure
 - Linux
 - Apache
 - Python
 - Kerberos ACL allows the service principal the web service runs as to create and manage user principals
- Web service design will serve as a model for integrating other unsupported applications

Integration with our Human Resources System

- At the time of the IdM POC PeopleSoft was our HR system
- Fermilab moved to WorkDay as stage 1 was in progress
 - Cloud based
 - Unsupported by D1 IdM
- WorkDay supports SCIM for integration
 - The version of D1 IdM being implemented does not
- Fermi staff created a WorkDay integration to transfer user data to a D1 IdM web service to create identities in IdM

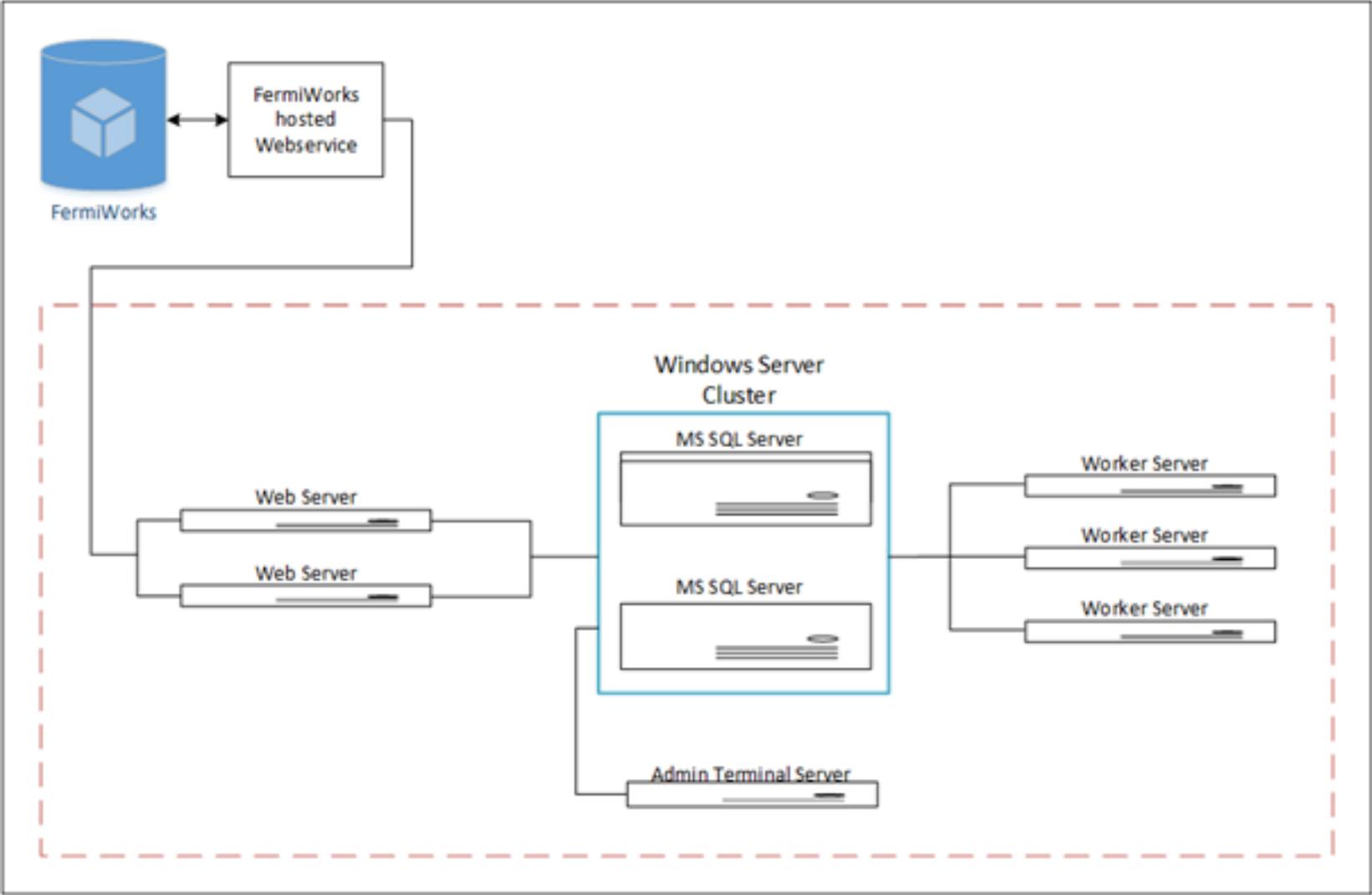
Integration with our Human Resources System



Development, Quality Assurance, and Production

- IdM is tightly integrated with WorkDay
- WorkDay has Test/Development, Quality Assurance, and Production environments
- We chose to emulate this for IdM
 - Fermi Phase 1 – Test/Development
 - Virtual servers
 - Fermi Phase 2 – QA
 - Emulate planned production environment
 - SQL Server cluster on physical hardware
 - Virtual servers for web interface and job servers
 - Fermi Phase 3 – Production
 - Same as QA

IdM Environment



Preparing for Production

- Build out production IdM service
- Build out production kadmin service
- Pass QA
- Connect to WorkDay
 - Import users
- Connect to Active Directories and Kerberos realm
 - Map users and set resources in IdM for accounts in AD and Kerberos
- Test Service Desk interface
- Test Computer Security interface
- Enable automated provisioning

Future Plans

- Integration with Service Now
 - IdM acts as an execution engine. All workflow decisions will be in Service Now
- Active Directory Permissions
 - Remove elevated access from users
- Fermi Phase 2
 - Implement attribute based roles
 - Mail lists
 - Data access
- Fermi Phase 3
 - Connect to additional service providers
 - Provision access to applications based on attributes or role assignment

Questions

- Al Lilianstrom – lilstrom@fnal.gov
- Dr. Olga Terlyga – terlyga@fnal.gov