



Operated by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

Authentication Services at Fermilab

Al Lilianstrom

Computer Security Awareness Day

November 2014

Abstract

- This talk will cover the authentication services available at Fermilab: Kerberos, Active Directory, LDAP, multi-factor authentication, federation and more, as well as a new project to manage digital identities.

-
- Authentication
 - Identity Management
 - What to Expect in the Future

Authentication

- Kerberos
- Active Directory
- LDAP
- KCA
- Eduroam
- Multi-factor
- Federation
 - ADFS
 - Shibboleth

Kerberos

- FNAL.GOV Realm
 - Recently upgraded to support stronger encryption methods
- Primarily used for logon authentication
 - Linux
 - Workstations
 - Servers
 - Farm nodes
 - OSX

Active Directory

- FERMI Domain
- Primarily used for logon authentication
 - Workstations
 - Windows 7
 - Windows 8
 - Servers
 - Windows 2003
 - Windows 2008
 - Windows 2012
 - OSX
- Two way trust exists between the FNAL.GOV Kerberos Realm and the FERMI Windows Domain

LDAP

- aka SERVICES
- Used for FermiMail, FermiPoint, ServiceNow, and dozens of other web services
- Available to any application that supports LDAP authentication
- No trust exists between the LDAP Service and either the FERMI Domain or the FNAL.GOV Kerberos realm.

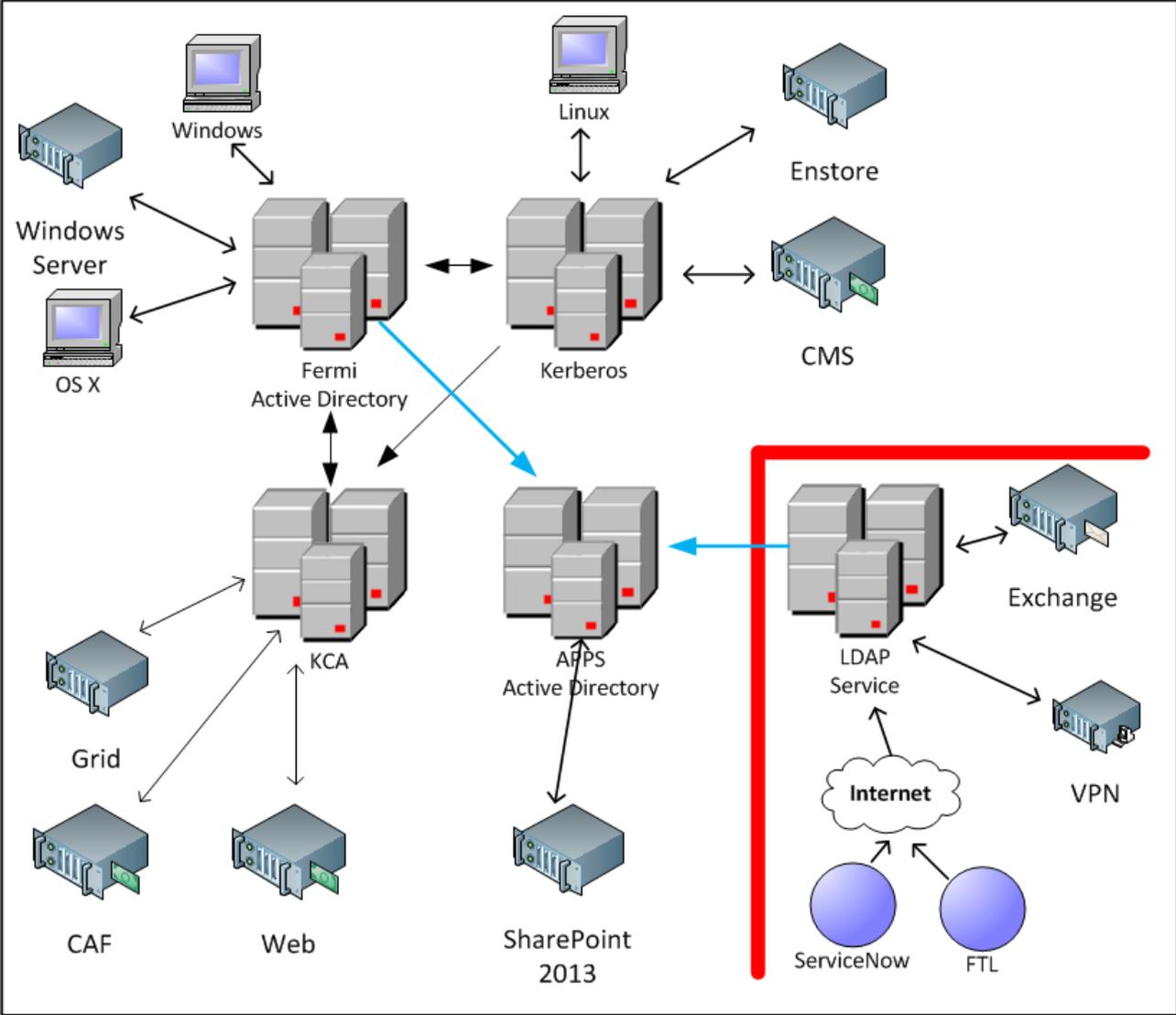
KCA Service

- Kerberos Certificate Authority
 - Short lifetime certificates for accessing web services
 - Kerberos Authentication
 - FNAL.GOV Realm
 - FERMI Domain
 - Clients
 - Get-Cert script
 - NetID Manager

APPS

- New service based on Windows Active Directory designed to let Service Providers allow access to their applications from either the FERMI domain or the LDAP service
- APPS trusts both the FERMI domain and the LDAP Service

The Big Picture



Eduroam

- Eduroam (**education roaming**) is the secure, world-wide roaming access service developed for the international research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions.
(<https://www.eduroam.us/>)
- Identity Provider on line and in production
- Radius based
 - Windows Server 2012
 - Network Policy Server
- Uses the LDAP Service for Authentication

Multi-Factor

- RSA SecurID
 - In production with
 - Administrative terminal servers
 - Domain administrators
 - Server administrators
 - Network administration
 - Remote Citrix access
 - FermiWorks administration
 - Linux Interactive Logons (SSH)

Federation

- ADFS
 - v2.1 in production
 - Based on Windows Server 2012
 - SharePoint Server 2013
 - ADFS solved authentication issues that arose based on our security configuration
 - SharePoint integrated applications
 - Office 365
 - Uses the LDAP Service for Authentication

Federation

- Shibboleth
 - Open Source
 - Service Provider
 - Currently in test on Apache and IIS
 - Identity Provider
 - Fermilab is working with Gluu (<http://www.gluu.org>)
 - Gluu to manage a on-premise high availability Shibboleth cluster for Fermilab
 - IdP Configuration
 - Integration with Service Providers
 - On Premise and in the Cloud
 - Gateway to InCommon
 - Uses the LDAP Service for Authentication

Federation

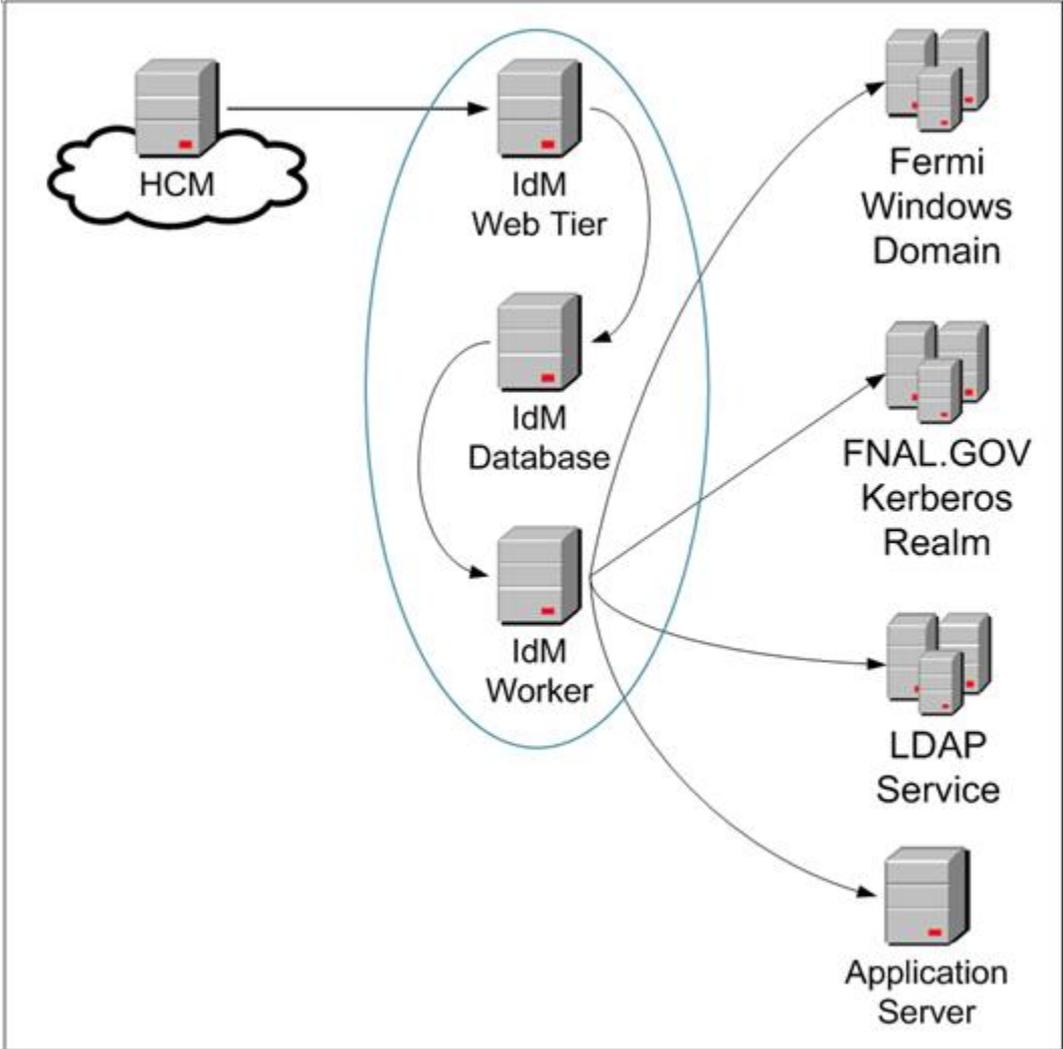
- ADFS and Shibboleth are for web applications
 - Applications that are authenticated by either will participate in a single sign on environment
 - Federation is authentication not authorization
 - The federated application will still need to grant the user access to the application
 - Participation in InCommon will allow simplified interaction between participating sites
 - Assuming proper authorization a user at a remote site would access Fermilab Federated resources with their local credentials – not a Fermilab username and password

Identity Management

- Dell Quest 1 Identity Management system
 - Implementation began Spring 2014
 - Currently in **Build and Test**
 - Connected to test Active Directory and Kerberos realms
 - Working on the interface to FermiWorks

- Next
 - Go Live and manage account lifecycle in central authentication services
 - Connect to Service Providers and move towards role based provisioning

Identity Management



Future Plans

- Authentication
 - Eduroam
 - Service Provider at Fermilab
 - Open wireless access will remain
 - Cloud
 - Extend central authentication to the cloud
 - Windows Domain Controllers
 - Kerberos Realm
 - LDAP Service
 - Federation

End

- Questions?
- Contact Information

Al Lilianstrom

lilstrom@fnal.gov