



Single Sign On at Fermilab

A Year of Change

Al Lilianstrom and Dr. Olga Terlyga

NLIT 2016

May 2nd, 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

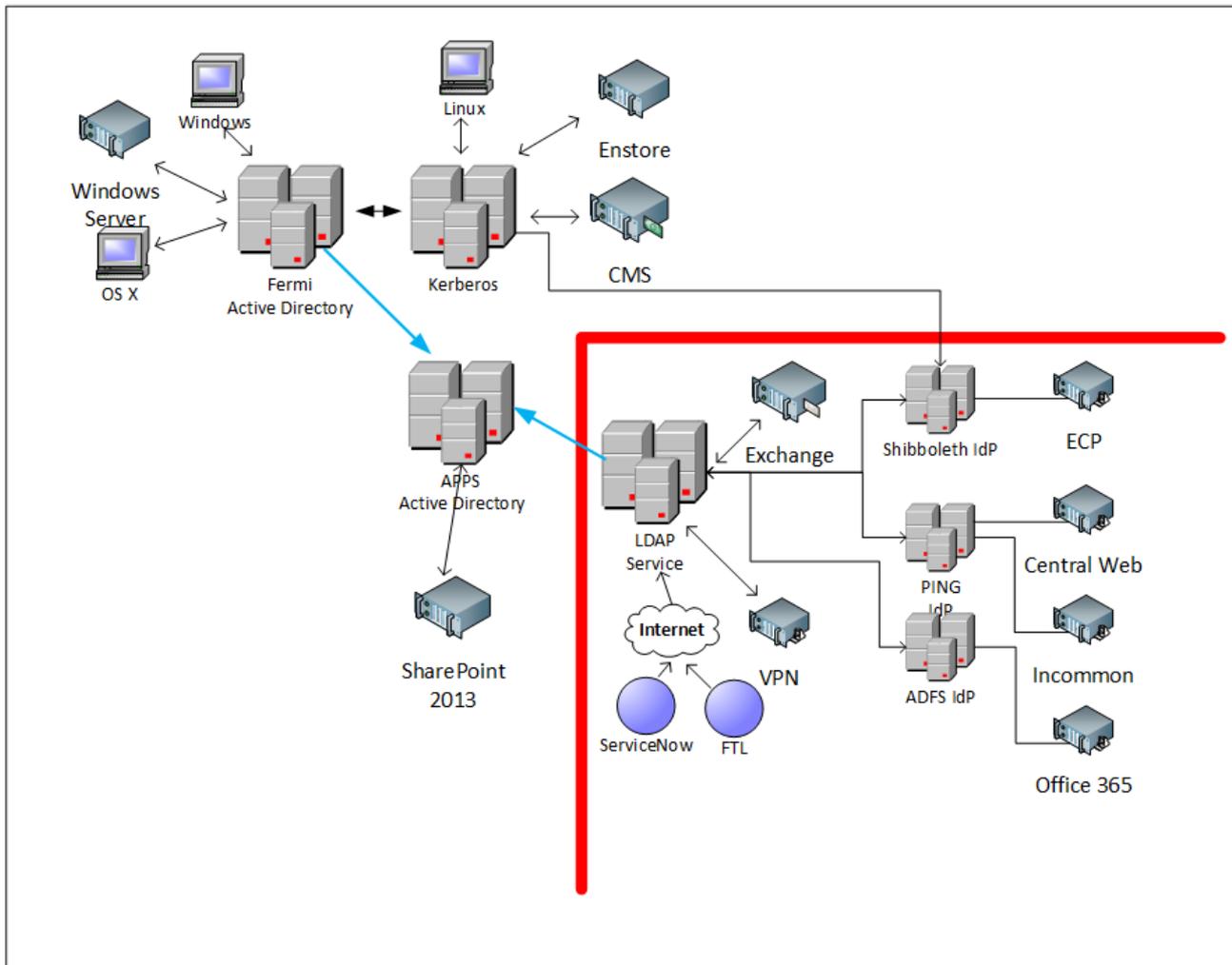
www.fnal.gov

Single Sign On at Fermilab - A Year of Change

The past year has seen a significant amount of change to the Single Sign On Service at Fermilab. Applications, configuration, integration - all designed to bring the service closer to a true single sign on environment to meet the needs for both our business and scientific computing users. This talk will cover these changes in detail and explain how they work in the unique Fermilab environment.

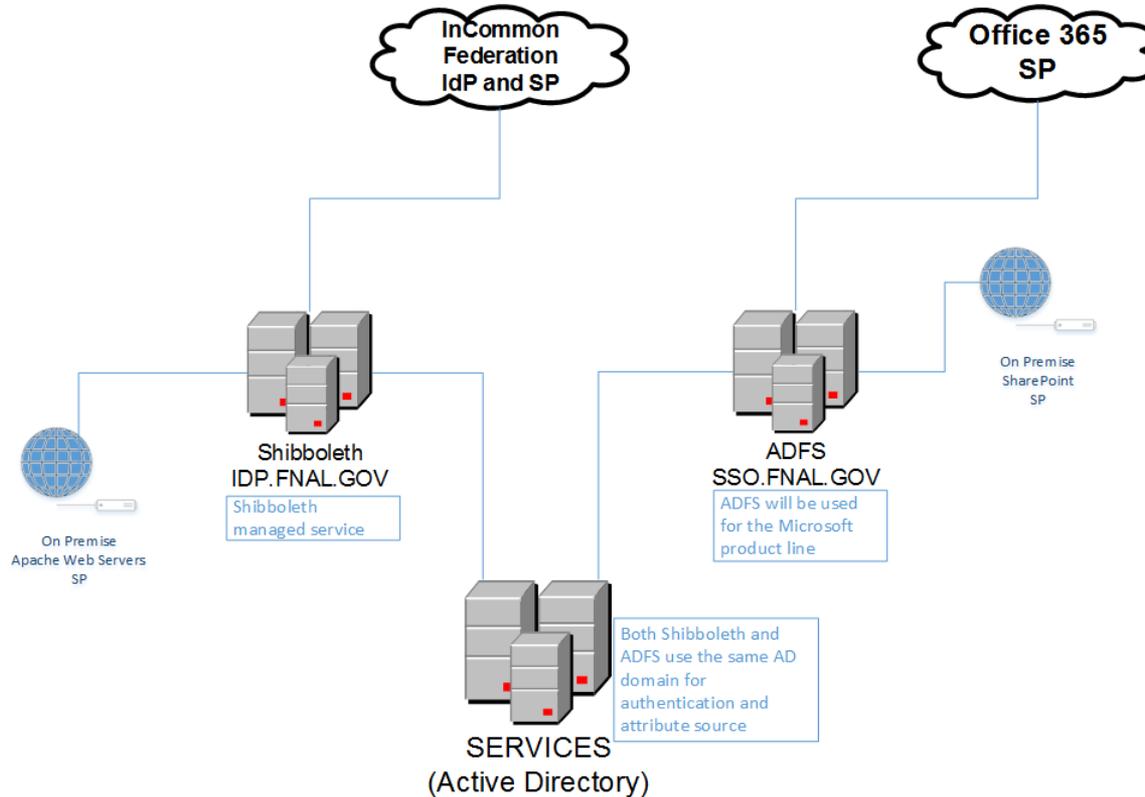
Topics include Shibboleth, PingFederate, ADFS, ECP, CILogon, Incommon, Active Directory, Kerberos, LDAP, and more

Our Authentication Realms



2015

- Twelve months ago the Single Sign On (SSO) environment looked like this:



- The fun was just about to begin

2015

- As shown in the previous slide SSO at Fermilab consisted of two distinct services
 - ADFS
 - Microsoft applications (SharePoint)
 - Office 365
 - Shibboleth
 - Apache web servers
 - InCommon
- Both services used the same Active Directory for authentication.

2015

- Shibboleth service
 - Managed remotely by a third party
 - Performance issues
 - Reliability issues
 - Configuration problems
 - GUI lacked flexibility
- Third party was moving out of management business
 - Advised us that significant price increases were coming

2015

- Alternatives
 - Shibboleth
 - SimpleSAMLphp
 - ADFS
 - Cloud Applications
 - Commercial On Premise Applications

- Considerations
 - Support
 - Future applications

Alternatives

- Shibboleth
 - Free*
 - Complicated configuration
 - Requires subject matter expert

- SimpleSAMLphp
 - Free*
 - Simple configuration
 - Presented on at NLIT in 2015
 - Documentation available
 - Concerns over support of future applications

Alternatives

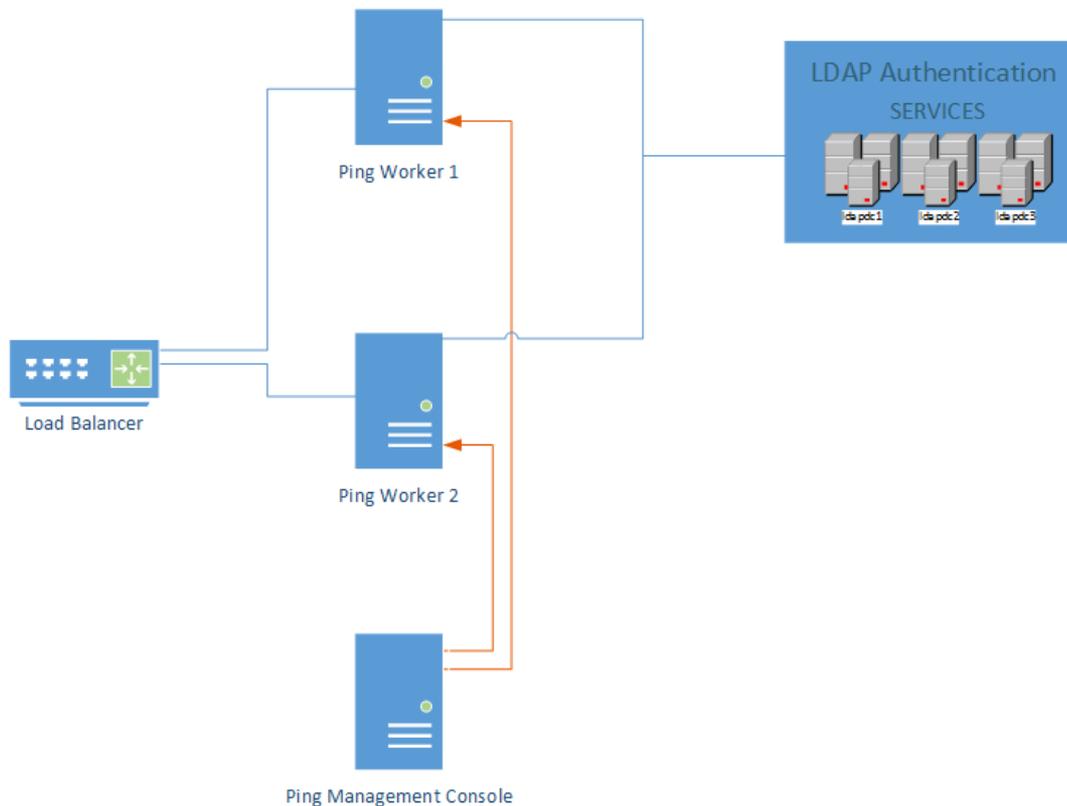
- ADFS
 - In use at Fermilab
 - Supported for all current applications
 - Concerns over support of future applications
- Cloud Applications
 - Concerns over moving core infrastructure outside of our network
 - Concerns over flexibility
 - Concerns over support of future applications

Alternatives

- Commercial Applications
 - Fermilab had previously investigated commercial software
 - Cost
 - Market review was conducted
 - Software was evaluated
- Our Choice
 - PingFederate was chosen to replace the Shibboleth service
 - Some concerns over support of future applications

Replacing Shibboleth

- PingFederate service design
 - Two worker nodes
 - One management console

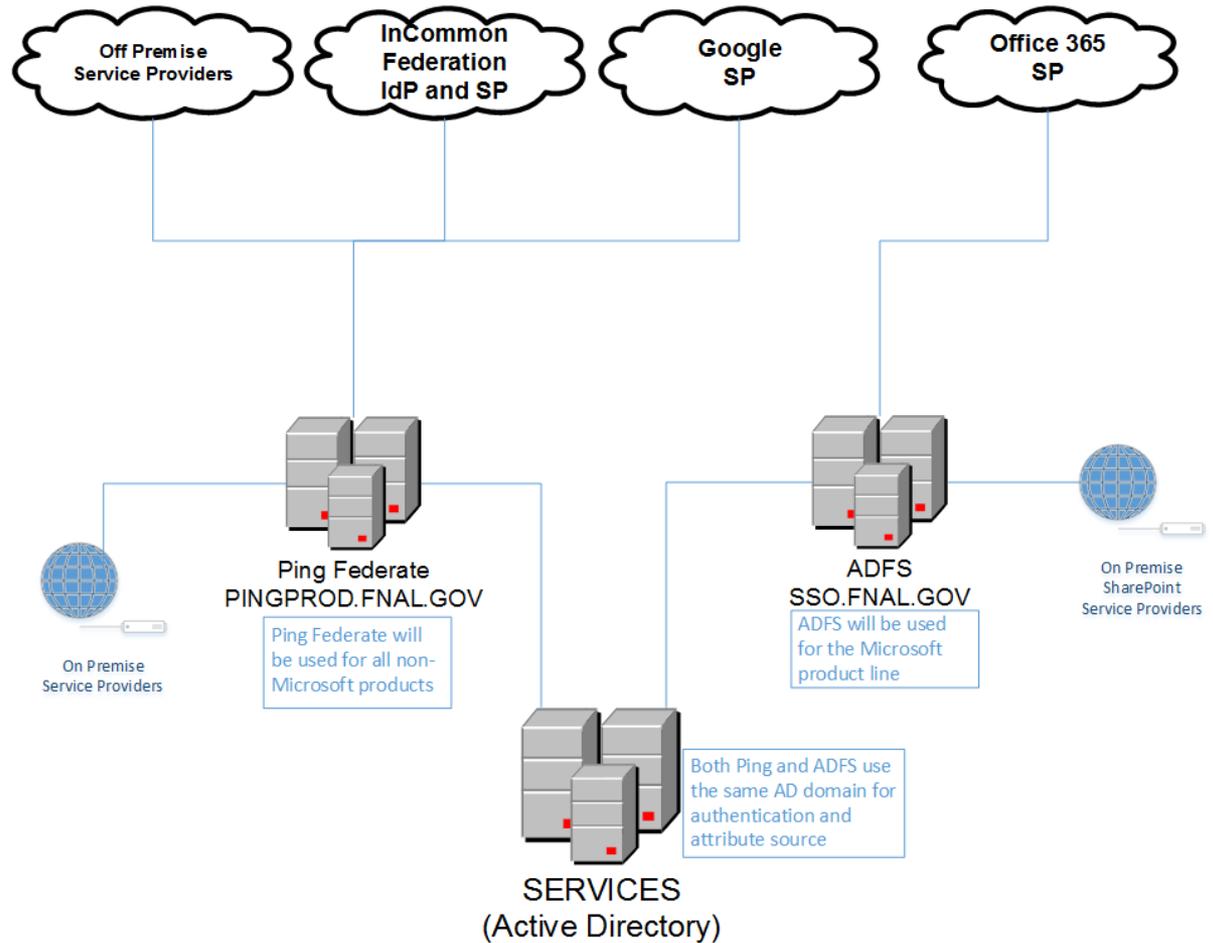


Migration to PingFederate – Service Providers

- Shibboleth-based Service Providers
- InCommon
 - PingFederate was not able to consume metadata from URL
 - PingFederate was not able to consume metadata aggregates
 - Connections needed to be configured individually.
 - Scoped attributes required small manual edit of IdP metadata
 - eduPersonTargetedID changed, requiring users to re-register with Service Providers
 - Tom Scavo and Jim Basney at InCommon provided valuable assistance
- Able to utilize API to insert and configure connections
 - Script created to add Service Providers

Interoperability

- Two federation services
 - ADFS
 - PingFederate
 - Common authentication service

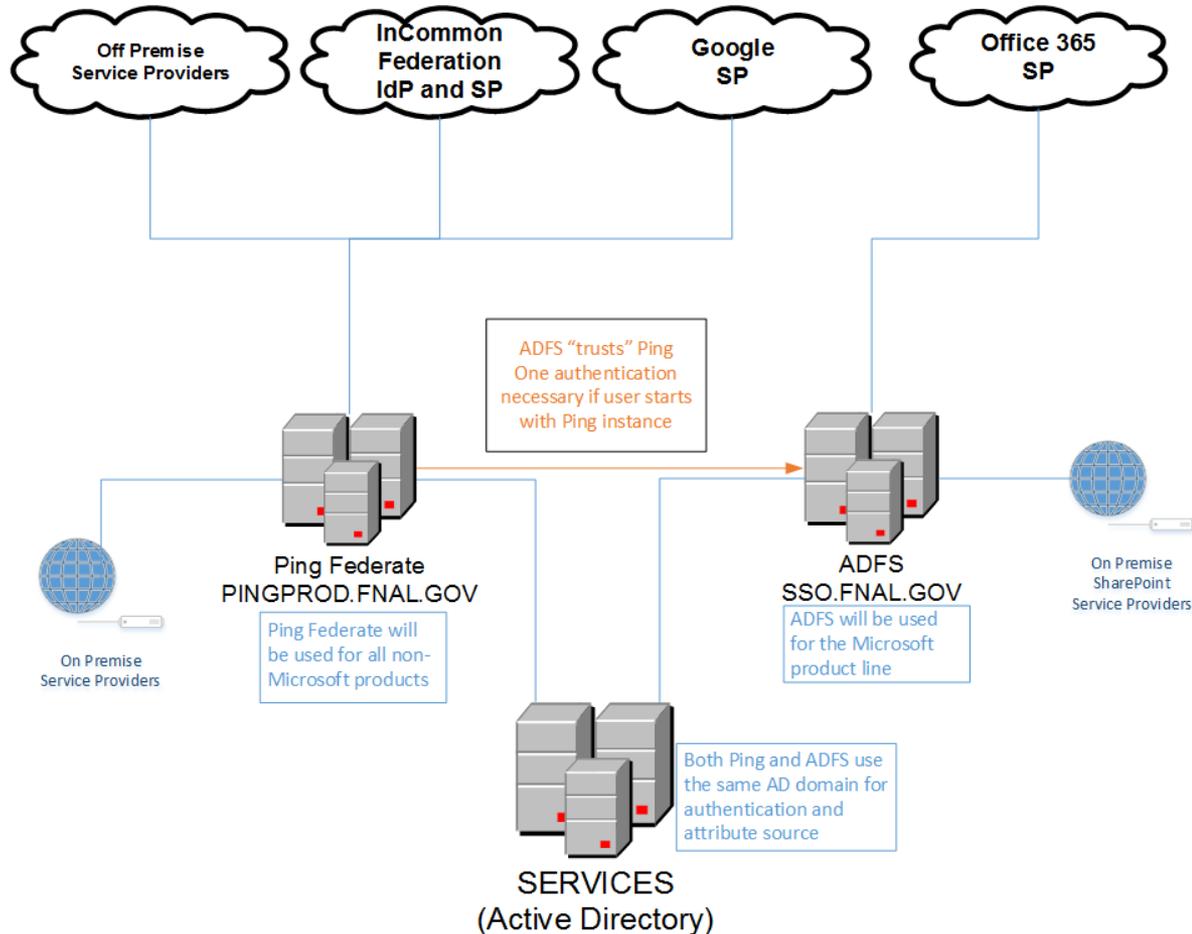


Interoperability

- Two logins required if accessing services managed by both federation servers
 - Establish trust between the two services
- Configuration
 - ADFS
 - Relying Party Trust
 - Identity Provider Trust
 - PingFederate
 - Identity Provider Trust
 - Relying Party Trust
 - Each PingFederate Service Provider requires additional configuration

Interoperability

- Single logon
 - Almost...



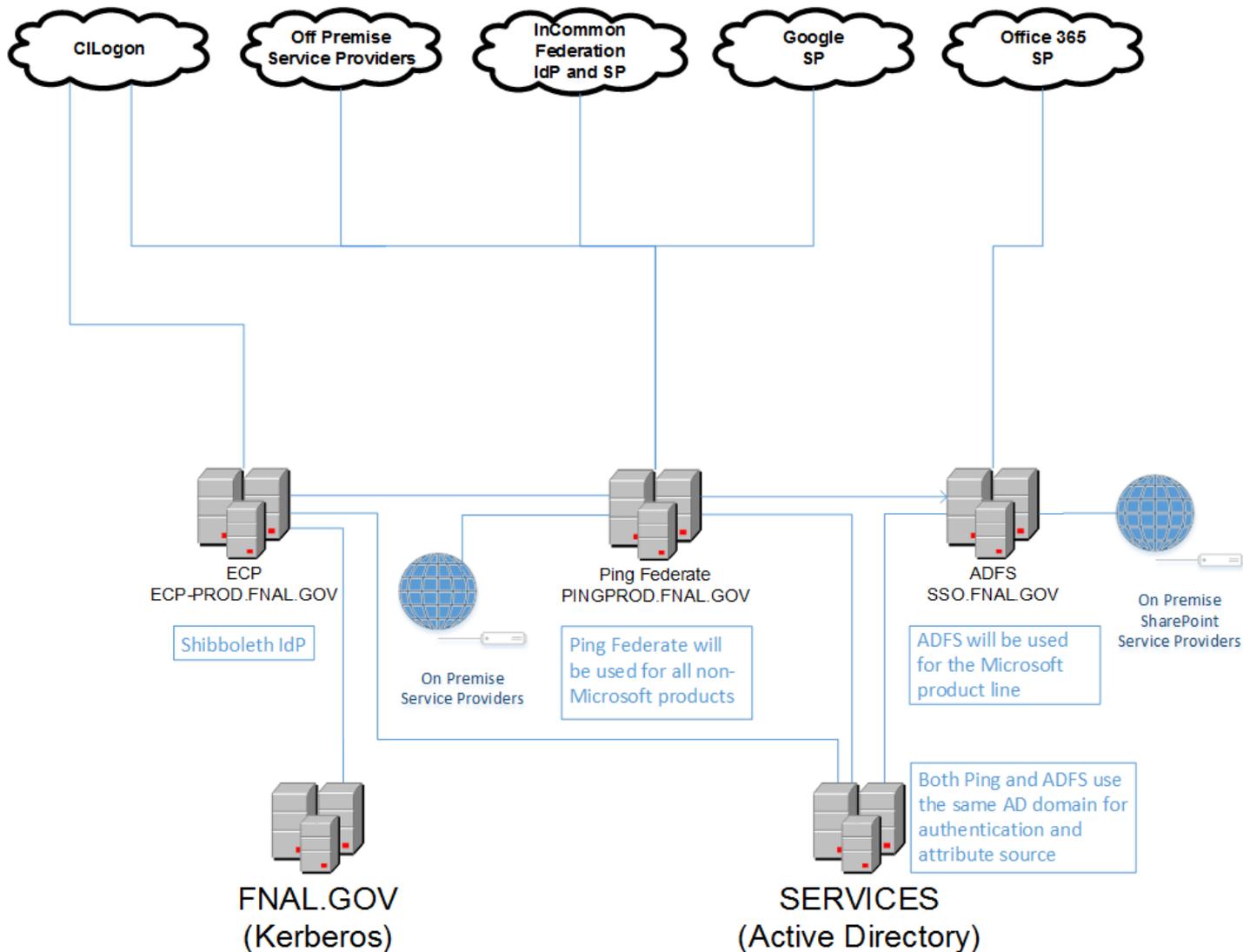
ECP

- Scientific Computing at Fermilab requested support of Enhanced Client or Proxy (ECP)
 - (<https://wiki.shibboleth.net/confluence/display/CONCEPT/ECP>)
 - It is the profile of SAML authentication designed for clients other than browsers, such as:
 - desktop applications
 - server-side code running in a web application
 - just about anything else that's not a browser
- Not supported by PingFederate or ADFS
- Requires a Shibboleth server
 - Integrated with our existing PingFederate service
 - PingFederate is our gateway to InCommon

ECP

- Shibboleth v2.4.0
- Kerberos and Username/Password authentication on two different endpoints
- ECP only, no token authentication
- Same signing certificate as PingFederate
- Supports compound Kerberos principals mapped to a person used in automated processes (user/cron/somenode.fnal.gov)

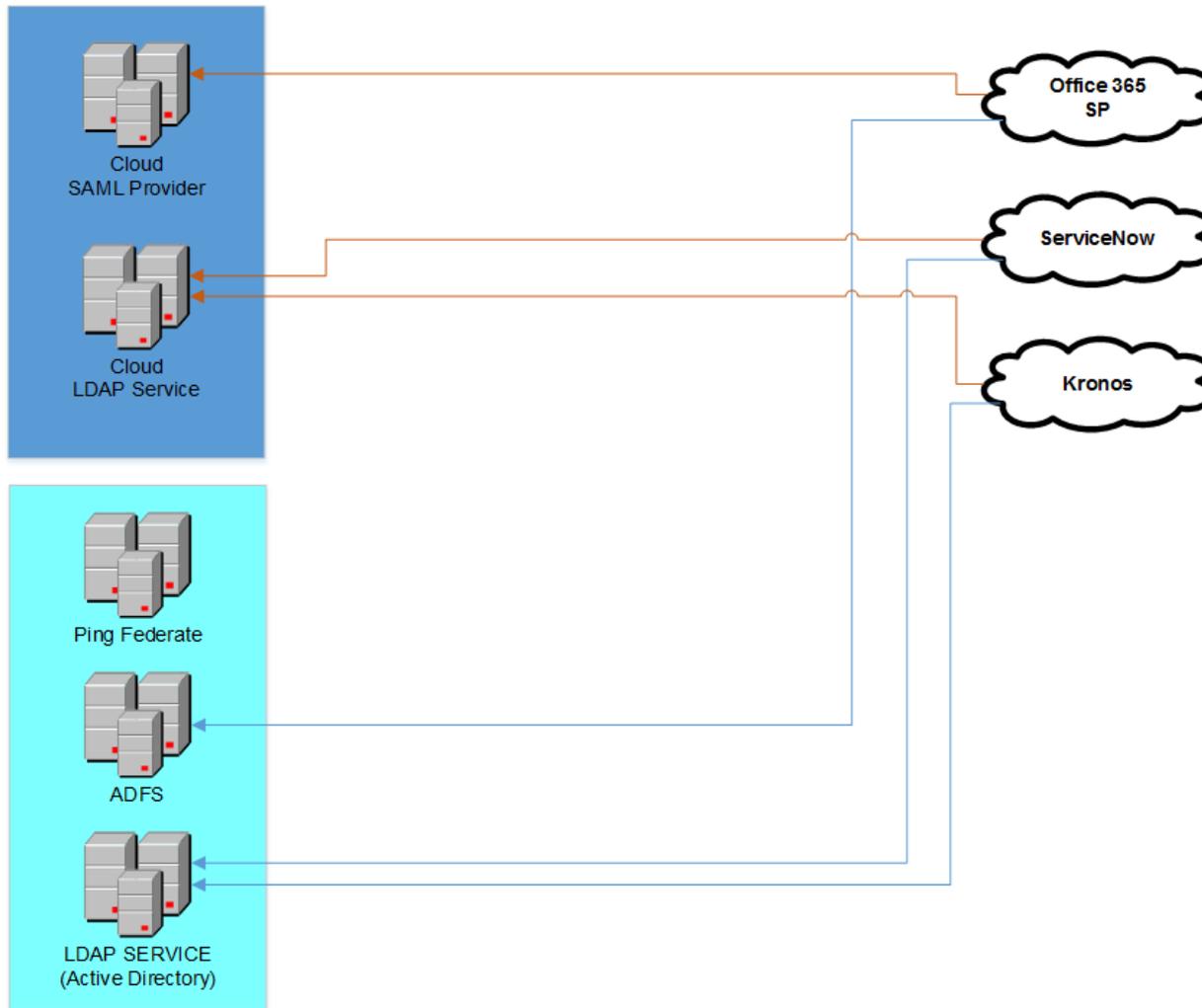
Federation Now



Next

- Kerberos authentication
- The majority of cloud based services in use at Fermilab use on-premise authentication
- Recent events have shown the need for cloud based authentication services for cloud based services
- Fermilab is currently prototyping an extension of our on-premise federation services into the cloud for use by our cloud services

Next – Cloud Authentication



Questions

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

Single Sign On and Federation

A Birds of a Feather Discussion

- Facilitators: Al Lilianstrom and Dr. Olga Terlyga
- NLIT 2016
- May 2nd, 2106

Single Sign On and Federation - Birds of a Feather

There are ongoing efforts at some of the national laboratories - working towards single sign on (SSO) of web applications for their users. This talk is not really a talk. It is meant to be a discussion session among the administrators of the SSO applications working towards a goal of regular email exchanges and monthly phone conferences among interested parties - not just to advance SSO at the individual laboratories - but to work towards federating access between the labs.

Single Sign On and Federation - Birds of a Feather

- Discussion topics include
 - SSO software
 - Target applications
 - Authentication services
 - Cloud Services
 - Identity Providers
 - Service Providers

Single Sign On and Federation - Birds of a Feather

- Goals
 - Ongoing discussion between the labs
 - Mail list
 - Monthly Phone Conference
 - Presentations?