Person Directory Service - Spring 2020 server replacement

What

IAM is upgrading the OpenLDAP software and replacing servers for eds.u.washington.edu (Person Directory Service - PDS).

When

We are targeting June 18th, 2020 as our migration date. We're asking PDS customers to complete testing by June 12th.

Why

- Maintain access to community support by using a recent OpenLDAP version
- OS of current cluster is approaching end of life (Centos 6)
- Updates to newer version of mdb (lmdb) storage technology

Who needs to take action?

Developers and support teams that are still using PDS (eds.u.washington.edu) should to test their applications against the newer PDS eval environment wh ich is available via **eds-eval.u.washington.edu**.

What do I need to do?

1. Test to your application and configuration against eds-eval.u.washington.edu to see if any changes are needed
2. Send an email to iam-support@uw.edu with the subject "Person Directory Service" once you have verified your test environment can to connect to the PDS evaluation environment: eds-eval.u.washington.edu.
3. Report any problems you have testing to iam-support@uw.edu before June 13th.

Note: eds-eval.u.washington.edu is a copy of yesterday's production data.

What is changing?

Several of the software components supporting the PDS cluster has been updated. This includes new Linux OS, new OpenSSL libraries, newer OpenLDAP version.

The PDS service is critical to a handful of core functions of the University. Our traditional strategy for the PDS environment has been to make changes very carefully.

- **New OS**: Servers go from Centos 6 to Centos 7. Due to changes in data center strategy our geographic diverse server node is hosted in GCP Oregon instead of the UW leased space at the Tierpoint datacenter. The Linux platform team expects to vacate Tierpoint by 2023.
- **New OpenSSL libraries**: Few differences between Centos 6 and Centos 7 for TLS.
- **New OpenLDAP software**: OpenLDAP goes from 2.4.44 to 2.4.47.
- **Server Certificate**: Unchanged. During the last upgrade in 2016 we had to change the server certificate to InCommon because several Windows Stunnel clients would not trust the old UWCA root certificate while using the latest TLS capabilities.
- **Replication strategy**: Unchanged. Data is updated in near real-time from the Identity Registry.

Additional questions..

eds-eval results so far?

eds-eval.u.washington.edu was upgraded on in January. No complaints have been received and normal uses of eds-eval continue to appear in the access reports.

LDAP design changes?

No, the PDS LDAP (OU) structure is identical between the old and new PDS environments.

What were the last changes made to the PDS environment?

See the previous communication page: Person Directory Service - Summer 2016 server replacement

Which environments have already been tested?

As June 17th, 2020 the following environments have successfully connected to eds-eval:

- idp.u.washington.edu

- www.ehs.washington.edu
- devapp-sislibrary.admin.washington.edu (student team)
- bobhurt.cac.washington.edu
- mailman1.u.washington.edu
- Stunnel via legacy PWS connection tester (simpleexternal)
- Stunnel via Softerra LDAPBrowser 4.5 (EXTERNAL)
- uwitconcert-dev.s.uw.edu (Concert/EDMS team)

Why is the service still using OpenLDAP software?

IAM will retire PDS in the future. OpenLDAP has provided excellent performance and reliability but is limiting in support of modern data structures and APIs. All new customer requests for person data have been directed to use the Person Web Service (PWS). New features and attributes are being or have been added to PWS and will not be made available via the legacy LDAP interface.

If PDS is going away and new customers haven't been admitted isn't it a lot of overhead to have customers migrate to PWS?

Many customers have been directed to use PWS or other interfaces to get person data. Only a handful of uses are left and several are in the process of migrating off PDS. The list of remaining integrations left to migrated off PDS is small (list below). When critical uses of PDS are migrated to other interfaces we will either remove resiliency capabilities or work directly with remaining customers to migrate off LDAP.

IAM integrations

- idp.u.washington.edu (PWS in evaluation)
- netid.washington.edu

Customer integrations (remaining as of May 29th, 2020)

- uwitconcert*.s.uw.edu (concert team)
- app-sislibrary.admin.washington.edu
- mailman1.u.washington.edu (replacement project underway)
- ldapmgmt.cac.washington.edu (work underway to deprecate)
- catalysttools.washington.edu
- rice.kuali.washington.edu (concert team)
- www.ehs.washington.edu
- oars.ehs.washington.edu
- csde.washington.edu (client now migrated to PWS)
- oea.washington.edu
- wheels.u.washington.edu (migrating to PWS)